Benutzerhandbuch - Deutsch

FUJITSU Software ServerView Suite

Remote Management

iRMC - integrated Remote Management Controller

Ausgabe Juni 2009

Kritik… Anregungen… Korrekturen…

Die Redaktion ist interessiert an Ihren Kommentaren zu diesem Handbuch. Ihre Rückmeldungen helfen uns, die Dokumentation zu optimieren und auf Ihre Wünsche und Bedürfnisse abzustimmen.

Sie können uns Ihre Kommentare per E-Mail an manuals@ts.fujitsu.com senden.

Zertifizierte Dokumentation nach DIN EN ISO 9001:2000

Um eine gleichbleibend hohe Qualität und Anwenderfreundlichkeit zu gewährleisten, wurde diese Dokumentation nach den Vorgaben eines Qualitätsmanagementsystems erstellt, welches die Forderungen der DIN EN ISO 9001:2000 erfüllt.

cognitas. Gesellschaft für Technik-Dokumentation mbH
www.cognitas.de

Copyright und Handelsmarken

Copyright © 2009 Fujitsu Technology Solutions GmbH.

Alle Rechte vorbehalten.
Liefermöglichkeiten und technische Änderungen vorbehalten.

Alle verwendeten Hard- und Softwarenamen sind Handelsnamen und/oder Warenzeichen der jeweiligen Hersteller.

Inhalt

1 Einleitung 13

1.1 Zielgruppen und Zielsetzung des Handbuchs 15
1.2 Funktionen des iRMC (Überblick) 16
1.3 Kommunikationsschnittstellen des iRMC 21
1.4 IPMI - Technischer Hintergrund 22
1.5 Änderungen gegenüber der vorherigen Ausgabe 31
1.6 Darstellungsmittel 32

2 Zum ersten Mal am iRMC anmelden 33

2.1 Voraussetzungen 33
2.2 iRMC-Voreinstellungen 34
2.3 An der iRMC-Web-Oberfläche anmelden 35

3 iRMC konfigurieren 37

3.1 LAN-Schnittstelle des iRMC konfigurieren 38
3.1.1 Voraussetzungen 39
3.1.1.1 An der richtigen LAN-Schnittstelle gesteckt? 39
3.1.1.2 Zusammenspiel der IP-Adressen des iRMC und des Systems 40
3.1.1.3 Zugriff aus einem anderen Sub-Netz 40
3.1.2 LAN-Schnittstelle konfigurieren: Konfigurationstools 40
3.1.3 LAN-Schnittstelle über das BIOS Setup konfigurieren 41
3.1.4 LAN-Schnittstelle testen 43

3.2 Text-Konsolumleitung via LAN über das BIOS Setup konfigurieren 44
3.2.1 Text-Konsolumleitung konfigurieren 45
3.2.2 Konsolumleitung bei laufendem Betriebssystem nutzen 48

3.3 Die serielle Schnittstelle des iRMC konfigurieren und nutzen 50
3.3.1 Die serielle Schnittstelle konfigurieren 51
3.3.2 Benutzeroberfläche Remote Manager (Serial) nutzen 53

3.4 iRMC über die iRMC-Web-Oberfläche konfigurieren 54
3.4.1 LAN-Parameter konfigurieren 54
3.4.2 Alarmbenachrichtigung (Alerting) konfigurieren 55
3.4.3 Text-Konsolumleitung konfigurieren 55

3.5 iRMC über den Server Configuration Manager konfigurieren 56
3.5.1 LAN-Parameter konfigurieren 56
3.5.2 Alarmbenachrichtigung (Alerting) konfigurieren 57

4 Benutzerverwaltung für den iRMC 59

4.1 Konzept der Benutzerverwaltung für den iRMC 60

4.2 Benutzerberechtigungen 62

4.3 Lokale Benutzerverwaltung für den iRMC 64
4.3.1 Lokale Benutzerverwaltung über die iRMC-Web-Oberfläche 64
4.3.2 Lokale Benutzerverwaltung über den Server Configuration Manager 66

4.4 Globale Benutzerverwaltung für den iRMC 68
4.4.1 Überblick 69
4.4.2 iRMC-Benutzerverwaltung mithilfe eines LDAP Directory Service (Konzept) 70
4.4.2.1 Globale Benutzerverwaltung über die OU „iRMCgroups“ . . . 70
4.4.2.2 Server-übergreifende globale Benutzerberechtigungen 72
4.4.2.3 Einstellungen für die bevorzugte Shell 75
4.4.3 Struktur „iRMCgroups“ im LDAP Directory Service generieren . . 76
4.4.3.1 LDIF-Datei erstellen 76
4.4.3.2 LDIF-Datei in den Directory Service importieren 79
4.4.4 iRMC-Benutzerverwaltung via Microsoft Active Directory 80
4.4.4.1 LDIF-Datei in Microsoft Active Directory importieren 80
4.4.4.2 LDAP/SSL-Zugriff des iRMC am Active Directory Server konfigurieren 86
4.4.4.3 iRMC-Benutzer der OU „iRMCgroups“ zuordnen 91

4.4.5 iRMC-Benutzerverwaltung via Novell eDirectory 98
4.4.5.1 Software-Komponenten und Systemanforderungen 98
4.4.5.2 Novell eDirectory installieren 99
4.4.5.3 Novell eDirectory konfigurieren 106
4.4.5.4 iRMC-Benutzerverwaltung in Novell eDirectory integrieren . 112
4.4.5.5 iRMC-Benutzer der OU „iRMCgroups“ zuordnen 120
4.4.5.6 Tipps zur Administration von Novell eDirectory 124
4.4.6 iRMC-Benutzerverwaltung via OpenLDAP 127
4.4.6.1 OpenLDAP installieren 127
4.4.6.2 SSL-Zertifikate erzeugen 127
4.4.6.3 OpenLDAP konfigurieren 128
4.4.6.4 iRMC-Benutzerverwaltung in OpenLDAP integrieren 129
4.4.6.5 Tipps zur Administration von OpenLDAP 132
4.4.7 SSL Copyright 134

5 Advanced Video Redirection 137

5.1 Voraussetzungen: Die Einstellungen für die AVR überprüfen 138

5.2 Advanced Video Redirection verwenden 139
5.2.1 Parallele AVR-Sitzungen 140
5.2.2 Local Monitor Off-Funktionalität 141
5.2.3 Umleitung der Tastatur 142
5.2.4 Umleitung der Maus 144
5.2.4.1 Mauszeiger synchronisieren 144
5.2.4.2 Verwalteter Windows Server: Einstellungen für Mauszeiger-Synchronisation anpassen 146
5.2.4.3 Verwalteter Linux Server: Einstellungen für Mauszeiger-Synchronisation anpassen 149

5.3 Menüs des AVR-Fensters 151
5.3.1 Menü Extras 152
5.3.2 Menü Remote Storage 155
5.3.3 Menü Languages 155
5.3.4 Menü Preferences 156

6 Remote Storage 159

6.1 Remote Storage am Remote-Arbeitsplatz bereitstellen . . . 160
6.1.1 Remote Storage starten 161
6.1.2 Speichermedien für Remote Storage bereitstellen 163
6.1.3 Speichermedien als Remote Storage verbinden 165
6.1.4 Remote Storage-Verbindungen trennen 167
6.1.5 Speichermedien entfernen 168

6.2 Remote Storage via Remote Storage Server bereitstellen . 169
6.2.1 Remote Storage Server installieren 170
6.2.2 Ausführungsmodi des Remote Storage Servers 175
6.2.3 Remote Storage Server konfigurieren, starten und beenden . . 176

7 iRMC-Web-Oberfläche 181

7.1 An der iRMC-Web-Oberfläche anmelden 182

7.2 Erforderliche Benutzerberechtigungen 184

7.3 Aufbau der Bedienoberfläche 187

7.4 System Information - Informationen zum Server 190
7.4.1 System Overview - Allgemeine Informationen zum Server . . 191
7.4.2 System Component Information -Informationen zu den Server-Komponenten 194

7.5 iRMC - Informationen, Firmware und Zertifikate 195
7.5.1 iRMC Information - Informationen zum iRMC 196
7.5.2 Save iRMC Firmware Settings - Firmware-Einstellungen sichern 200
7.5.3 Certificate Upload - DSA/RSA-Zertifikat und privaten DSA/RSA-Schlüssel laden 202
7.5.4 Generate a self-signed RSA Certificate -Selbstsigniertes RSA-Zertifikat erzeugen 208

7.6 Power Management 210
7.6.1 Power On/Off - Server ein-/ausschalten 211
7.6.2 Power Options - Power Management des Servers konfigurieren 215
7.6.3 Power Supply Info - Stromversorgung und IDPROM-Daten der FRU-Komponenten 218

7.7 Sensors - Status der Sensoren überprüfen 219
7.7.1 Fans - Lüfter überprüfen 220
7.7.2 Temperature - Temperatursensoren überprüfen 222
7.7.3 Voltages - Spannungssensoren überprüfen 224
7.7.4 Power Supply - Stromversorgung überprüfen 225
7.7.5 Component Status - Status der Serverkomponenten überprüfen 226

7.8 System Event Log (SEL) - Event-Log des Servers anzeigen und konfigurieren 227
7.8.1 System Event Log Content - Information zum SEL und SEL-Einträge anzeigen 228
7.8.2 System Event Log Configuration - SEL konfigurieren 231

7.9 Server Management Information - Server-Einstellungen konfigurieren 233

7.10 Network Settings - LAN-Parameter konfigurieren 239
7.10.1 Network Interface - Ethernet-Einstellungen des iRMC konfigurieren 240
7.10.2 Ports and Network Services - Ports und Netzdienste konfigurieren 243
7.10.3 DHCP Configuration - Host-Namen für den iRMC konfigurieren 247
7.10.4 DNS Configuration - DNS für den iRMC aktivieren 249

7.11 Alerting - Alarmbenachrichtigung konfigurieren 251
7.11.1 SNMP Trap Alerting - SNMP-Alarmweiterleitung konfigurieren . 252
7.11.2 Serial / Modem Alerting - Alarmweiterleitung über Modem konfigurieren 254
7.11.3 Email Alerting - E-Mail-Benachrichtigung konfigurieren 256

7.12 User Management - Benutzerverwaltung 263
7.12.1 iRMC User - lokale Benutzerverwaltung am iRMC 263
7.12.1.1 New User Configuration - Neuen Benutzer konfigurieren . . 265
7.12.1.2 User '<name>' Configuration - Benutzerkonfiguration (Details) 266
7.12.2 Directory Service Configuration (LDAP) - Directory Service am iRMC konfigurieren 273

7.13 Console Redirection - Konsolumleitung 281
7.13.1 BIOS Text Console - Text-Konsolumleitung konfigurieren und starten 281
7.13.1.1 Bios Console Redirection Options - Text-Konsolumleitung konfigurieren 283
7.13.1.2 Text Console Redirection (via Serial Over LAN) - Text-Konsolumleitung starten 285
7.13.1.3 Text-Konsolumleitung bei laufendem Betriebssystem 290
7.13.2 Advanced Video Redirection - Advanced Video Redirection (AVR) starten 292

7.14 Remote Storage 300

7.15 iRMC über Telnet / SSH (Remote Manager) bedienen 302

8 iRMC über Telnet/SSH (Remote Manager) bedienen 307

8.1 iRMC über das ServerView Remote Management Frontend bedienen 308

8.2 Remote Manager 309
8.2.1 Remote Manager bedienen 309
8.2.2 Menü-Übersicht 310
8.2.3 Anmeldeprozess 312
8.2.4 Hauptmenü des Remote Manager 314
8.2.5 Erforderliche Benutzerberechtigungen 316
8.2.6 Passwort ändern 317
8.2.7 System Information - Informationen zum verwalteten Server . . 318
8.2.8 Power Management 319
8.2.9 Enclosure Information - System Event-Log und Status der Sensoren 321
8.2.10 Service Processor - IP-Parameter, Identifizierungs-LED und Reset des iRMC 325
8.2.11 Console Redirection (EMS/SAC) - Text-Konsolumleitung starten 326
8.2.12 Start a Command Line shell... - SMASH CLP Shell starten . . 327
8.2.13 Command Line Protocol (CLP) 328

9 iRMC via Server Configuration Manager konfigurieren . . . 333

9.1 Systemkonfiguration starten . . . 334
9.1.1 Server Configuration Manager über den Installation Manager aufrufen . . . 334
9.1.2 Server Configuration Manager über das Windows Startmenü aufrufen . . . 335
9.1.3 Server Configuration Manager über den Operations Manager aufrufen . . . 337

9.2 ASR&R Fan Settings . . . 342

9.3 ASR&R Temperature Settings . . . 344

9.4 iRMC LAN Interface - LAN-Einstellungen des iRMC konfigurieren . . . 346

9.5 iRMC Networking Ports - Ports und Netzdienste konfigurieren . . . 349

9.6 iRMC DNS Registration - Host-Namen für den iRMC konfigurieren . . . 351

9.7 iRMC DNS Server - DNS für den iRMC aktivieren . . . 353

9.8 iRMC EMail Alerting - E-Mail-Weiterleitung konfigurieren . . . 355

9.9 iRMC Mail Format Settings - Mail-Format-abhängige Einstellungen . . . 358

9.10 iRMC SNMP Alerting - SNMP-Alarm-Weiterleitung konfigurieren . . . 360

9.11 iRMC User Management - Lokale Benutzerverwaltung am iRMC . . . 361

9.12 iRMC Directory Service - Directory Service konfigurieren . 367
9.12.1 iRMC für Microsoft Active Directory konfigurieren . . . 369
9.12.2 iRMC für Novell eDirectory / OpenLDAP konfigurieren . . . 371

9.13 iRMC Advanced Features - Remote Storage Server, License Key und HP SIM-Integration . . . 374

10 Firmware-Update 377

10.1 Firmware des iRMC (Überblick) 378

10.2 USB Memory Stick erstellen 381

10.3 Online-Update 384
10.3.1 Online-Update via ServerView Update Manager 384
10.3.2 Online-Update via ServerView Update Manager Express oder ASP 385
10.3.3 Online-Update mit den Betriebssystem-Flash-Tools 385

10.4 Offline-Update 387
10.4.1 Offline-Update via ServerView Update Manager 387
10.4.2 Offline-Update über das Menü der FlashDisk 388
10.4.3 Offline-Update mit dem Flash-Tool flbmc 389

10.5 Emergency Flash 390

10.6 Flash-Tools 391

11 Remote-Installation des Betriebssystems via iRMC 395

11.1 Betriebssystem via iRMC installieren - generelles Vorgehen 396

11.2 Speichermedium als Remote Storage verbinden 398

11.3 Verwalteten Server von der PRIMERGY ServerView Suite DVD 1 booten und via Installation Manager konfigurieren . 402

11.4 Betriebssystem nach Konfiguration auf dem verwalteten Server installieren 409
11.4.1 Windows nach Konfiguration auf dem verwalteten Server installieren 409
11.4.2 Linux nach Konfiguration auf dem verwalteten Server installieren 413

12 IPMI OEM-Kommandos 419

12.1 Überblick 419

12.2 Beschreibung der IPMI OEM-Kommandos 421
12.2.1 Beschreibungsformat 421
12.2.2 SCCI-konforme Power On/Off-Kommandos 422
12.2.3 SCCI-konforme Kommunikationskommandos 427
12.2.4 SCCI-konformes Signalkommando 429
12.2.5 Firmware-spezifische Kommandos 430
12.2.6 BIOS-spezifische Kommandos 434
12.2.7 iRMC-spezifische Kommandos 436

Literatur 445

Stichwörter 451

1 Einleitung

Moderne Serversysteme werden zunehmend komplexer. Entsprechend steigen auch die Anforderungen an das Management dieser Systeme.

Als Reaktion auf diese Entwicklung gründeten einige Hersteller die Initiative „Intelligent Platform Management Interface (IPMI)“ mit dem Ziel der Definition einer standardisierten, abstrakten und Mitteilung-basierten Schnittstelle zwischen dem zentralen System-Controller (Baseboard Management Controller - BMC) und intelligenter Hardware zum Plattform-Management. Näheres zu IPMI finden Sie im Abschnitt „IPMI - Technischer Hintergrund“ auf Seite 22.

Der iRMC (**i**ntegrated **R**emote **M**anagement **C**ontroller) ist ein BMC mit integriertem LAN-Anschluss und erweiterter Funktionalität, die bisher nur durch zusätzliche Einsteckkarten, wie z. B. das RemoteView Service Board (RSB), angeboten wurde. Auf diese Weise ermöglicht der iRMC die umfassende Kontrolle von PRIMERGY Servern, unabhängig vom Systemstatus, insbesondere also auch die Kontrolle von PRIMERGY Servern, die sich im „out-of-Band“-Systemstatus befinden.

Bild 1: iRMC auf der Systembaugruppe eines PRIMERGY Servers

Als autonomes System auf der Systembaugruppe eines aktuellen PRIMERGY Servers verfügt der iRMC über ein eigenes Betriebssystem, einen eigenen Web-Server sowie eine eigene Benutzerverwaltung und ein eigenständiges Alarm-Management. Der iRMC wird auch im Stand-by-Betrieb des Servers mit Strom versorgt.

Im vorliegenden Handbuch werden Konfiguration und Bedienoberflächen des iRMC beschrieben.

1.1 Zielgruppen und Zielsetzung des Handbuchs

Das Handbuch wendet sich an Systemverwalter, Netzverwalter und Service-Fachleute, die über fundierte Hard- und Software-Kenntnisse verfügen. Es vermittelt Grundkenntnisse zur IPMI-Technologie und informiert ausführlich über folgende Themen:

- Anmelden am iRMC
- Konfiguration des iRMC
- Benutzerverwaltung am iRMC
- Advanced Video Redirection via iRMC
- Remote Storage via iRMC
- iRMC-Web-Oberfläche
- Telnet/SSH-basierte Oberfläche (Remote Manager) des iRMC
- Konfiguration des iRMC über den Server Configuration Manager
- Firmware-Update
- Remote-Installation des Betriebssystems via iRMC
- IPMI OEM-Kommandos

Weitere Dokumentation zum ServerView Remote Management

Weitere Handbücher zum ServerView Remote Management-Umfeld und zur PRIMERGY ServerView Suite finden Sie im Kapitel „Literatur“ auf Seite 445.

Service

Falls Sie weitere Fragen zum Remote Management für PRIMERGY-Server haben, wenden Sie sich an Ihren zuständigen Service und Supportpartner.

Weitere Informationen

http://www.ts.fujitsu.com

1.2 Funktionen des iRMC (Überblick)

Der iRMC unterstützt eine Vielzahl von standardmäßig angebotenen Funktionen sowie mit Advanced Video Redirection (AVR) und Remote Storage zwei zusätzliche advanced Features für das Remote Management von PRIMERGY Servern. Für die Nutzung von AVR und Remote Storage benötigen Sie einen gültigen License Key, den Sie käuflich erwerben können.

Standardfunktionalität des iRMC

- Browser-Zugang

  Der iRMC verfügt über einen eigenen Web-Server, der von der Management-Station über einen Standard Web-Browser angesprochen werden kann.

- Sicherheit (SSL, SSH)

  Der Zugang zum Web-Server kann, ebenso wie die grafische Konsolumleitung inklusive Maus und Tastatur, über HTTPS/SSL abgesichert werden. Für den Zugriff auf den iRMC über den Remote Manager kann eine kryptographisch gesicherte Verbindung eingerichtet werden, die durch die Mechanismen von SSH abgesichert ist. Der Remote Manager ist eine alphanumerische Bedienoberfläche des iRMC.

- ServerView-Integration

  Die ServerView-Agenten erkennen den iRMC und ordnen ihn automatisch dem betreffenden Server zu. Damit lässt sich die iRMC-Web-Oberfläche ebenso wie die Text-Konsolumleitung über das ServerView Remote Management Frontend direkt aus dem ServerView Operations Manager heraus starten.

- Power Management

  Unabhängig vom Systemzustand haben Sie folgende Möglichkeiten, vom Remote-Arbeitplatz aus den verwalteten Server ein- und auszuschalten:

  – über die iRMC-Web-Oberfläche
  – über den Remote Manager und das Command Line Interface (CLP)
  – per Script

- Text-Konsolumleitung

  Über das ServerView Remote Management Frontend können Sie eine Telnet/SSH-Session zum iRMC initiieren. Es wird dann der Remote Manager aufgerufen, über den Sie eine Text-Konsolumleitung starten können.

- Grundfunktionen eines BMC

  Der iRMC unterstützt die Grundfunktionen eines BMC wie Spannungsmonitoring, Event-Logging und Recovery-Kontrolle.

- „Headless“ Systembetrieb

  Maus, Monitor und Tastatur sind am verwalteten Server nicht erforderlich. Daraus resultieren Vorteile, wie niedrigere Kosten, wesentlich einfachere Verkabelung im Rack und höhere Sicherheit.

- Identifizierungs-LED

  Zur einfacheren Identifizierung eines Systems, z.B. in einem voll ausgebauten Rack, können Sie über die iRMC-Web-Oberfläche die Identifizierungs-LED einschalten.

- Gobal Error-LED

  Eine Global Error-LED informiert Sie jederzeit über den Status des verwalteten Systems.

- LAN

  Bei einigen Systemen ist die LAN-Schnittstelle der eingebauten System-NIC (Network Interface Card) des Servers dediziert für das Management LAN reserviert. Bei anderen Systemen können Sie diese LAN-Schnittstelle per Konfiguration wahlweise

  – für das Management LAN reservieren,
  – für den „Shared“-Betrieb mit dem System einrichten oder
  – ganz dem System zur Verfügung stellen.

  Dem iRMC zugeordnet sind die Ports, die mit dem Symbol eines Schraubenschlüssels gekennzeichnet ist (siehe Bild 7 auf Seite 39).

- Command Line Interface (CLP)

  Der iRMC unterstützt neben dem Remote Manager auch das von der DMTF (Distributed Management Task Force) standardisierte SMASH CLP (**S**ystem **M**anagement **A**rchitecture for **S**erver **H**ardware **C**ommand **L**ine **P**rotocol)

- Einfache Konfiguration - interaktiv oder Script-basiert

  Für die Konfiguration des iRMC stehen Ihnen folgende Tools zur Auswahl:

  – iRMC-Web-Oberfläche
  – Server Configuration Manager
  – Server Management-Tool IPMIVIEW
  – BIOS Setup

  Die Konfiguration via Server Configuration Manager oder IPMIVIEW können Sie auch Script-basiert durchführen. Auf diese Weise kann bei der ersten Konfiguration des Servers mit ServerStart auch der iRMC konfiguriert werden. Auch die gleichzeitige Konfiguration einer größeren Anzahl von Servern lässt sich Skript-basiert durchführen.

- Lokale Benutzerverwaltung

  Der iRMC verfügt über eine eigene Benutzerverwaltung, mit der bis zu 16 Benutzer mit Passwörtern angelegt und je nach Gruppenzugehörigkeit mit unterschiedlichen Rechten versehen werden können.

- Globale Benutzerverwaltung mithilfe eines Directory Service

  Die globalen Benutzerkennungen für den iRMC werden zentral abgelegt im Verzeichnis (Directory) eines Directory Service. Auf diese Weise lassen sich die Benutzerkennungen auf einem zentralen Server verwalten und können somit von allen iRMCs verwendet werden, die mit diesem Server im Netz verbunden sind.

  Für die iRMC-Benutzerverwaltung werden zurzeit folgende Directory Services unterstützt:

  – Microsoft® Active Directory
  – Novell® eDirectory
  – OpenLDAP

- DNS / DHCP

  Der iRMC unterstützt die automatische Netz-Konfiguration. Er hat einen Default-Namen, und DHCP-Unterstützung ist standardmäßig eingestellt, sodass der iRMC seine IP-Adresse vom DHCP-Server erhält. Der iRMC-Name wird vom Domain Name Service (DNS) registriert. Es werden bis zu fünf DNS-Server unterstützt. Falls DNS/DHCP nicht verfügbar ist, unterstützt der iRMC auch statische IP-Adressen.

- Stromversorgung

  Die Stromversorgung des iRMC erfolgt über die Stand-by-Versorgung des Systems.

- Alarm-Management

  Das Alarm-Management des iRMC bietet folgende Möglichkeiten für die Weiterleitung von Alarmen (Alerting):

  – Platform Event Traps (PET) werden via SNMP versendet.

  – Direkte Benachrichtigung per E-Mail.

  – An die serielle Schnittstelle lässt sich ein Modem anschließen, über das Alarme (Alerts) versendet werden (z.B. per SMS an ein Mobiltelefon).

  Darüber hinaus versorgt der iRMC den ServerView-Agenten mit allen relevanten Informationen.

- System Event Log (SEL) auslesen, filtern und speichern.

  Den Inhalt des SEL können Sie filtern, einsehen, speichern und löschen

  – über die iRMC-Web-Oberfläche oder
  – über die Telnet-basierte Schnittstelle (Remote Manager) des iRMC.

Erweiterte Funktionalität des iRMC

Neben der Standardfunktionalität unterstützt der iRMC zusätzlich die Funktionen Advanced Video Redirection und Remote Storage.

- Advanced Video Redirection (AVR)

  Der iRMC unterstützt die Advanced Video Redirection mit folgenden Vorteilen:

  – Bedienung über einen Standard-Web-Browser. Auf der Management-Station braucht außer dem Java Runtime Environment keine zusätzliche Software installiert zu werden.

  – System-unabhängige Weiterleitung von Grafik- und Text-Konsole (einschließlich Maus und Tastatur).

  – Fernzugriff für Boot-Überwachung, BIOS-Administration und Bedienung des Betriebssystems.

- AVR bietet bis zu zwei gleichzeitige „virtuelle Verbindungen“ für das Arbeiten an einem Server von einem anderen Standort aus. Außerdem minimiert AVR die Netzbelastung durch Hardware- und Video-Komprimierung.
- Local Monitor Off-Unterstützung: Während einer AVR-Sitzung kann der lokale Bildschirm des verwalteten PRIMERGY Servers ausgeschaltet werden, um Unbefugte daran zu hindern, Eingaben und Aktionen der AVR -Sitzung am Server-lokalen Bildschirm zu verfolgen.

- Remote Storage

  Remote Storage stellt dem verwalteten Server ein „virtuelles“ Laufwerk zur Verfügung, das sich physisch am Remote-Arbeitsplatz befindet oder mithilfe eines Remote Storage Servers zentral im Netz bereitgestellt wird.

  Die per Remote Storage verfügbaren „virtuellen“ Laufwerke sind vergleichbar den lokalen Laufwerken einfach zu verwalten und bieten folgende Möglichkeiten:

  - Daten lesen und schreiben.
  - Von RemoteStorage booten.
  - Treiber und kleinere Anwendungen installieren.
  - BIOS Update vom Remote-Arbeitsplatz durchführen (BIOS Update per USB)

  Für die Bereitstellung eines „virtuellen“ Laufwerks am Remote Arbeitsplatz unterstützt Remote Storage folgende Gerätetypen:

  - CD-ROM
  - DVD-ROM
  - Memory Stick
  - Disketten-Image
  - CD ISO-Image
  - DVD ISO-Image

  Ein Remote Storage Server stellt ein ISO Image zentral im Netz als „virtuelles“ Laufwerk zur Verfügung.

  Remote Storage ermöglicht alternativ die gleichzeitige Anbindung von bis zu zwei „virtuellen“ Laufwerken am Remote Arbeitsplatz oder die Bereitstellung eines ISO Image via Remote Storage Server.

1.3 Kommunikationsschnittstellen des iRMC

Der iRMC bietet folgende Kommunikationsschnittstellen:

- **iRMC-Web-Oberfläche (Web-Schnittstelle)**

  Die Verbindung zum iRMC-Web-Server erhalten Sie über einen Standard-Web-Browser (z. B. Microsoft Internet Explorer, Mozilla Firefox).

  Über die Web-Oberfläche des iRMC haben Sie u.a. Zugriff auf alle Systeminformationen und Informationen der Sensoren wie Lüfterdrehzahlen, Spannungen etc. Sie können die Text-basierte Konsolumleitung konfigurieren oder die grafische Konsolumleitung (Advanced Video Redirection, AVR) starten. Darüber hinaus kann der Administrator die komplette Konfiguration des iRMC über die Web-Schnittstelle abwickeln. Der Zugang zum Web-Server des iRMC kann über HTTPS/SSL abgesichert werden.

  Die Bedienung des iRMC über die Web-Oberfläche ist beschrieben im Kapitel „iRMC-Web-Oberfläche“ auf Seite 181.

- **Remote Manager: Text-basierte Telnet/SSH-Oberfläche über LAN**

  Den Remote Manager können Sie wahlweise aufrufen

  – über das ServerView Remote Management Frontend,
  – direkt über einen Telnet/SSH-Client.

  Über die alphanumerische Bedienoberfläche des Remote Manager haben Sie u.a. Zugriff auf System-und Sensorinformationen, das Power Management und den Error-Eventlog. Außerdem können Sie die Text-Konsolumleitung sowie eine SMASH CLP Shell starten. Wenn Sie den Remote Manager über SSH (Secure Shell) aufrufen, ist die Verbindung zwischen Remote Manager und verwaltetem Server kryptographisch gesichert.

  Die Bedienung des iRMC über den Remote Manager ist beschrieben im Kapitel „iRMC über Telnet/SSH (Remote Manager) bedienen“ auf Seite 307.

- **Remote Manager (Serial): Text-basierte Schnittstelle über Serial 1**

  Die Oberfläche des Remote Manager (Serial) ist identisch mit der Oberfläche des Remote Manager.

1.4 IPMI - Technischer Hintergrund

Über die IPMI-Schnittstelle stellt der iRMC die BMC-Funktionalität zur Verfügung.

Intelligent Platform Management

Die Initiative „Intelligent Platform Management“ ist eine Reaktion auf die ansteigende Komplexität moderner Serversysteme. Zahlreiche Hersteller haben sich in dieser Initiative zusammengeschlossen, um eine neue Lösung für die Überwachung dieser Serversysteme zu erarbeiten.

Der Begriff „Intelligent Platform Management“ bringt den Kernaspekt dieses Lösungsansatzes zum Ausdruck: Funktionen zum Überwachen und Wiederherstellen von Systemen werden direkt in die Hard- und Firmware für das Plattform-Management implementiert.

Ziel

Ziel war die Definition einer standardisierten, abstrakten und Mitteilung-basierten Schittstelle zwischen dem zentralen System-Controller (Baseboard Management Controller - BMC) und intelligenter Hardware zum Plattform-Management.

Dabei fassten die Standardisierungsgremien die zentralen Charakteristika verschiedener Baugruppen zum Plattform-Management in standardisierende Beschreibungen.

Definition

Die IPMI-Spezifikation definiert:

> „IPMI is a hardware level interface specification that is ’management software neutral’ providing monitoring and control functions that can be exposed through standard management software interfaces such as DMI, WMI, CIM, SNMP, etc. As a hardware level interface, it sits at the bottom of a typical management software stack“ [siehe Abschnitt „IPMI und andere Management-Standards“ auf Seite 23].

Vorteil

Die IPMI-Spezifikationen sichern die Unabhängigkeit der Funktionen zu Inventory, Logging, Recovery und Überwachung eines Systems vom Prozessor, BIOS oder Betriebssystem des Systems.

Damit kann ein System auch in das Plattform-Management einbezogen werden, wenn es heruntergefahren und ausgeschaltet ist.

IPMI und andere Management-Standards

Am besten kann IPMI genutzt werden in Verbindung mit einer Software zum System-Management, die unter dem Betriebssystem läuft. Mit der Integration der IPMI-Funktionalität in die Managementfunktionalität, die eine Management-Applikation und das Betriebssystem bieten, entsteht eine mächtige Umgebung zum Plattform-Management.

Eine Übersicht zum Verhältnis von IPMI zum Management-Software-Stack zeigt Bild 2:

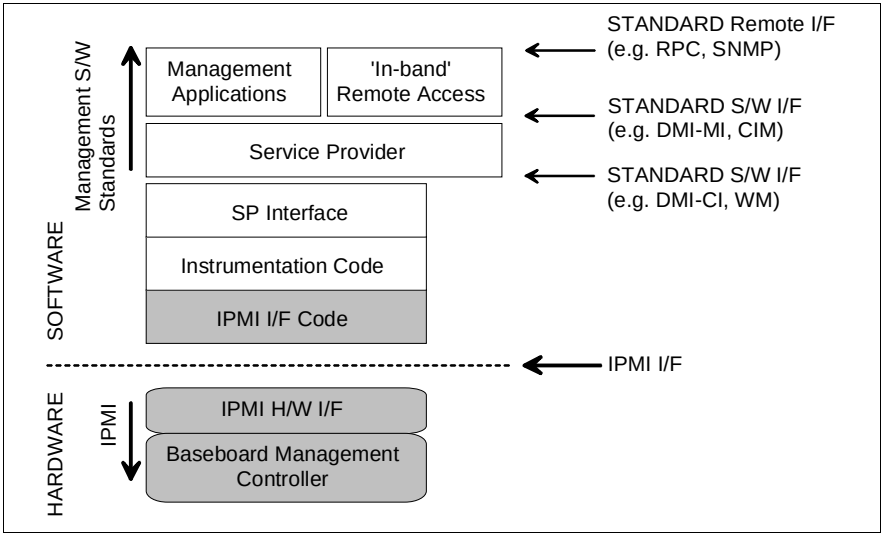


Bild 2: IPMI im Management-Software-Stack (Quelle: IPMI Specification, siehe Abschnitt „Referenzen“ auf Seite 30)

IPMI, IPMB und ICMB

Im Rahmen der IPMI-Initiative entstanden drei zentrale Standards:

– *IPMI. Intelligent Platform Management Interface Specification*
beschreibt die übergeordnete Architektur, die gängigen Kommandos, Ereignisformate, Datenpakete und Eigenschaften, die in IPMI-basierten Systemen zum Einsatz kommen.

– *IPMB. Intelligent Platform Management Bus*
ist ein I^2C-basierter (write only) Bus, der eine standardisierte Verbindung herstellt zwischen verschiedenen Baugruppen in einem Gehäuse.
Der IPMB kann auch als standardisierte Schnittstelle für Remote-Management-Baugruppen eingesetzt werden.

– *ICMB. Intelligent Chassis Management Bus*
(Derzeit im ServerView Remote Management-Umfeld nicht implementiert.)
bietet eine standardisierte Schnittstelle für den Austausch von Information zum Plattform-Management und zur Kontrolle zwischen Systemen. Der ICMB ist so entworfen, dass er mit einem Gerät implementiert werden kann, das an den IPMB angeschlossen wird.

IPMI Implementierung

Kernelement einer IPMI-Implementierung ist der Baseboard Management Controller (BMC).
Der BMC erfüllt folgende Aufgaben:

– Der BMC organisiert die Schnittstelle zwischen der Software für das System-Management und der Hardware für das Plattform-Management.

– Er bietet autonome Funktionen für die Überwachung, das Event-Logging und die Recovery-Kontrolle.

– Der BMC dient als Gateway zwischen der Software zum System-Management und IPMB.

IPMI ermöglicht das Erweitern von Plattform-Management: Über den IPMB können zusätzliche Management-Controller angebunden werden. Der IPMB ist ein I^2C-basierter serieller Bus, der zwischen den Hauptmodulen des Systems verläuft. Er wird für die Kommunikation mit und zwischen den Management-Controllern genutzt.

Mit der Unterstützung mehrerer Management-Controller bietet IPMI eine skalierbare Architektur: Ein komplexes Server-System kann mehrere Controller für die Überwachung verschiedener Subsysteme nutzen, z.B. der Stromversorgungen, der hot-swap RAID-Laufwerkseinschübe, usw.

Darüberhinaus bietet IPMI 'low-level' I^2C-Kommandos, mit denen über einen am IPMB angeschlossenen Management-Controller zugegriffen werden kann auf 'unintelligente' I^2C-Baugruppen, die keine IPMI-Kommandos verarbeiten.

Einen Überblick über die grundlegenden Elemente einer IPMI-Implementierung bietet Ihnen Bild 3 auf Seite 26.

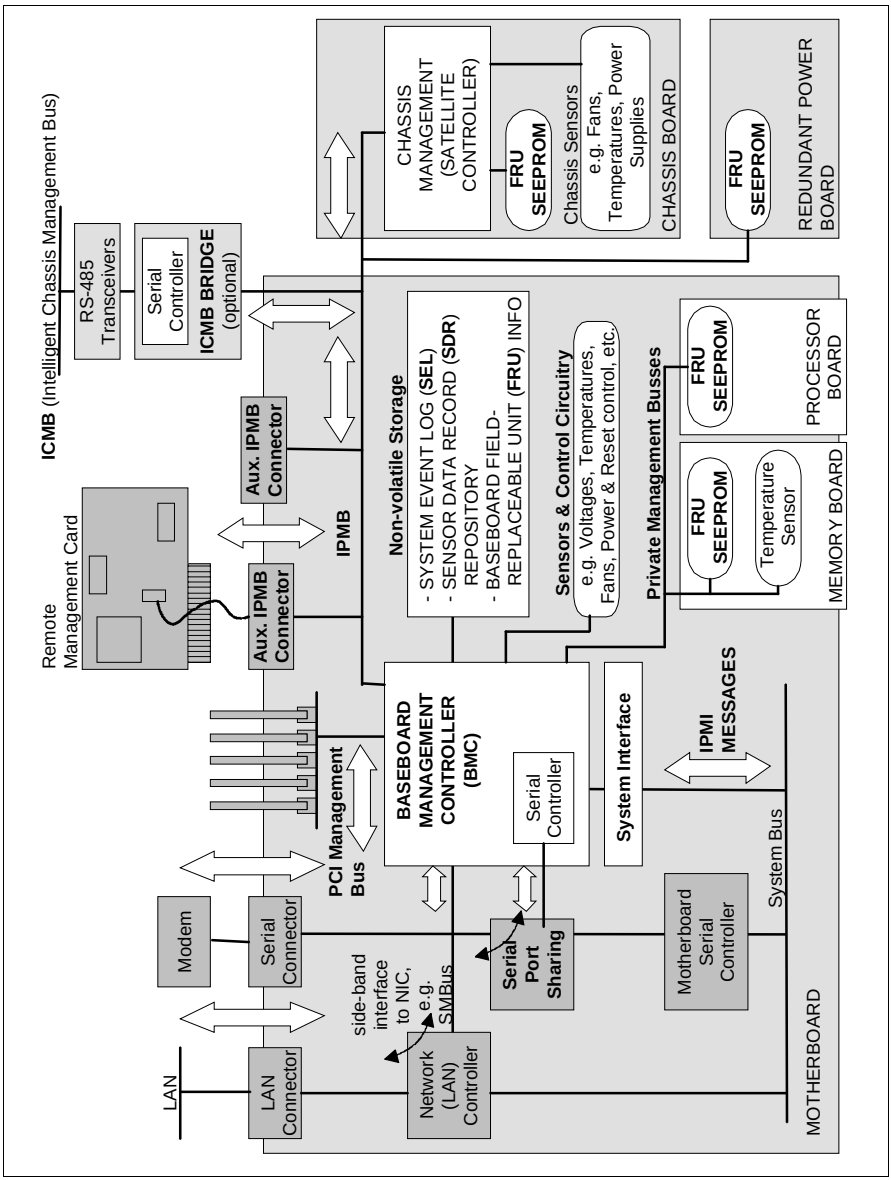


Bild 3: IPMI Blockdiagramm (Quelle: IPMI Specification, siehe Abschnitt „Referenzen“ auf Seite 30)

IPMI und „in-band“ und „out-of-band“ Management

Im System-Management-Umfeld wird unterschieden zwischen „in-band“-Management und „out-of-band“-Management:

– „in-band“-Management findet statt, wenn das Betriebssystem am verwalteten Server läuft.

– „out-of-band“-Management findet statt, wenn das Betriebssystem am verwalteten Server nicht läuft, z.B. weil Hardware defekt ist.

Mit den verschiedenen Schnittstellen, die ein IPMI-fähiges System zur Verfügung stellt, lassen sich IPMI-fähige Systeme sowohl „in-band“ als auch „out-of-band“ verwalten.

IPMI-over-LAN

"IPMI-over-LAN" ist die gängige Bezeichung für die Spezifikation der LAN-Schnittstelle im IPMI-Standard. Diese Spezifikation legt fest, wie IPMI-Mitteilungen an bzw. von dem BMC eines verwalteten Systems gesendet werden können - verkapselt in RMCP (Remote Management Control Protocol)-Datenpakete. Diese RMCP-Datenpakete werden übertragen über eine Ethernet-LAN-Verbindung über das UDP (User Datagram Protocol) unter IPv4 (Internet Protocol Version 4).

Das RMCP-Protokoll wurde spezifiziert, um das Management von Systemzuständen zu unterstützen, in denen das Betriebssystem nicht läuft. Das RMCP ist ein einfaches Frage-Antwort-Protokoll.

Die Schnittstelle für eine solche Verbindung wird bereitgestellt über einen onboard LAN-Controller, der dem BMC zugeordnet ist.

i Die Schnittstelle kann nur über einen onboard LAN-Controller zur Verfügung gestellt werden, nicht über eine gesteckte LAN-Karte.

Von den zwei Ports, die RCMP unter UDP nutzt, kommuniziert der BMC mit dem LAN-Controller über den Port 623 (Primary RMCP Port).

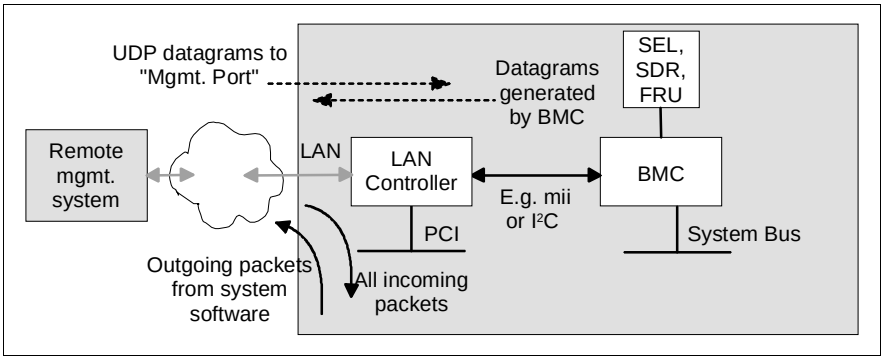


Bild 4: BMC und LAN-Controller

Serial Over LAN-Schnittstelle (SOL)

"Serial Over LAN" ist eine Schnittstelle im IPMI V2.0-Standard, die die Übertragung serieller Daten über eine LAN-Verbindung regelt. Im Einzelnen spezifiziert SOL dabei die Paketformate und Protokolle für den LAN-Transfer serieller Datenströme zwischen dem Serial Controller am verwalteten Rechner und einem Remote-Arbeitsplatz. SOL basiert auf der IPMI-over-LAN-Spezifikation.

Zur Einrichtung einer SOL-Verbindung initiiert eine Remote-Management-Anwendung zunächst eine IPMI-over-LAN-Session mit dem BMC. Danach können die SOL-Dienste vom Remote-Arbeitplatz aus aktiviert werden. Der Datenverkehr zwischen dem Serial Controller und dem Remote-Arbeitsplatz wird über dieselbe IPMI-Session abwickelt, über die auch die IPMI-Kommandos abgewickelt werden.

Sobald eine SOL-Verbindung eingerichtet ist, verläuft der Datentransfer zwischen Serial Controller und Remote Arbeitsplatz nach folgendem Schema:

– Transfer vom Serial Controller an den Remote-Arbeitsplatz:
  Der vom Serial Controller ausgehende Datenstrom wird vom BMC partitioniert, in Pakete "verpackt" und über LAN an den Remote-Arbeitsplatz gesendet.

– Transfer vom Remote-Arbeitsplatz an den Serial Controller:
  Die Zeichen, die in den vom Remote-Arbeitsplatz gesendeten Paketen enthalten sind, werden vom BMC entpackt und als Zeichenstrom an den Serial Controller weitergeleitet.

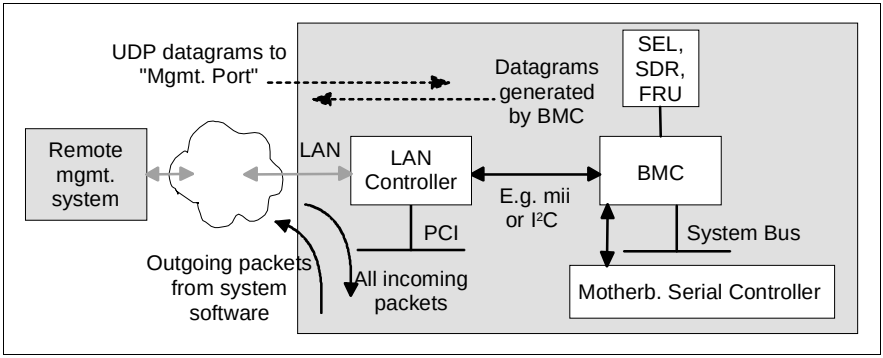


Bild 5: BMC und SOL

Die SOL-Zeichendaten werden als SOL-Mitteilungen zwischen dem BMC des verwalteten Systems und dem Remote-Arbeitsplatz ausgetauscht. Verkapselt in RMCP+-Datenpakete werden SOL-Mitteilungen in UDP Datagrammen übertragen über eine Ethernet-LAN-Verbindung unter IPv4 (Internet Protocol Version 4). Das RMCP+-Protokoll basiert auf dem RMCP-Protokoll, enthält jedoch Erweiterungen u.a. für Verschlüsselung und Authentifizierung.

Serial Over LAN ermöglicht "headless" Management durch Konsolumleitung sowohl des BIOS als auch des Betriebssystems des verwalteten Servers. Kostenintensive Konzentratorlösungen werden nicht benötigt.

Kanal-Konzept unter IPMI

'Kanäle' stellen die Mechanismen zur Verfügung, mit denen IPMI-Meldungen über verschiedene Verbindungsträger zum BMC geleitet werden. Es können bis zu neun Kanäle unterstützt werden. Die Systemschnittstelle und der Primary IPMB sind festgelegt. Die anderen sieben Kanäle stehen der Implementierung offen.

Kanäle können 'session-based' oder 'session-less' sein. Das Konzept 'Sitzung' hat zwei Zielrichtungen: Entweder ein Konzept zur Benutzer-Authentifizierung (siehe Abschnitt „Benutzerkennungen“ auf Seite 30) oder ein Konzept, um mehrere IPMI-Meldungs-Ströme über einen einzelnen Kanal zu leiten.

Beispiele für 'session-based' Kanäle sind LAN-Kanäle oder serielle oder Modem-Kanäle. Beispiele für 'session-less' Kanäle sind die Systemschnittstelle und der IPMB.

Benutzerkennungen

Für 'session-based' Kanäle (siehe Abschnitt „Kanal-Konzept unter IPMI“ auf Seite 29) ist eine Nutzeranmeldung notwendig. Die 'session-less' Kanäle haben dagegen keine Benutzer-Authentifizierung.

Unter IPMI ist die Konfiguration der Benutzer Kanal-spezifisch. So kann ein Benutzer verschiedene Rechte haben, je nachdem ob er auf den BMC über den LAN-Kanal oder über den seriellen Kanal zugreift.

Referenzen

Informationen zu den IPMI-Standards finden Sie im Internet:

http://developer.intel.com/design/servers/ipmi/index.htm

1.5 Änderungen gegenüber der vorherigen Ausgabe

Die vorliegende Ausgabe löst folgendes Online-Handbuch ab:
„iRMC - integrated Remote Management Controller“, Ausgabe November 2008.

Das Handbuch bietet folgende Neuerungen:

- iRMC-Web-Oberfläche:
  - Wichtige Einstellungen für die Anzeige der iRMC-Web-Oberfläche können über die Seite *iRMC Information* konfiguriert werden.
  - Für die Darstellung der iRMC-Web-Oberfläche im Ihrem Web-Browser können Sie zwischen zwei verschiedenen Farbschemata wählen.
- Kapitel „9 iRMC über den Server Configuration Manager konfigurieren“:

  SCU (Server Configuration Utility) heißt jetzt Server Configuration Manager. Das Layout der Benutzeroberfläche hat sich geringfügig geändert.
- Kapitel „10 IPMIVIEW“ entfällt. IPMIVIEW wird künftig in einem eigenen Handbuch beschrieben.
- Kapitel „11 Firmware-Update“:

  Zusätzliche Tools zur Aktualisierung der Firmware des iRMC:
  ServerView Update Manager Express und ASPs (Autonomous Support Packages)
- Kapitel „12 Remote-Installation des Betriebssystems via iRMC“:

  Beschreibung wurde aktualisiert für die Betriebssystem-Installation mithilfe des ServerView Installation Managers.

1.6 Darstellungsmittel

In diesem Handbuch werden folgende Darstellungsmittel verwendet:

Warnung!	Mit diesem Symbol wird auf Gefahren hingewiesen, die zu Gesundheitsgefährdung, Datenverlust und Geräteschäden führen können.
	Mit diesem Symbol werden wichtige Informationen und Tipps hervorgehoben.
►	Mit diesem Symbol wird ein Arbeitsschritt, den Sie ausführen müssen, dargestellt.
Kursive Schrift	Im Fließtext werden Kommandos, Menüpunkte, die Namen von Schaltflächen, Optionen, Dateinamen und Pfadnamen *kursiv* dargestellt.
<Schrift>	Kennzeichnet Variablen, die durch aktuelle Werte ersetzt werden müssen.
`dicktengleich`	Ausgaben des Systems werden `dicktengleich` dargestellt.
`dicktengleich halbfett`	Über die Tastatur einzugebende Anweisungen werden dicktengleich halbfett dargestellt.
[eckige Klammern]	Kennzeichnen optionale Eingaben.
{geschweifte Klammern}	Kennzeichnen eine Liste Alternativen, die durch „|“ voneinander getrennt sind.
Tastensymbole	Tasten werden entsprechend ihrer Abbildung auf der Tastatur dargestellt. Wenn explizit Großbuchstaben eingegeben werden sollen, so wird die Shift-Taste angegeben, z. B. SHIFT - A für A. Müssen zwei Tasten gleichzeitig gedrückt werden, so wird dies durch einen Bindestrich zwischen den Tastensymbolen gekennzeichnet.

Tabelle 1: Darstellungsmittel

Wird auf Textstellen in diesem Handbuch verwiesen, so wird die Überschrift des Kapitels bzw. Abschnitts genannt, wobei sich die Seitenangabe auf den Beginn des Abschnitts bezieht.

2 Zum ersten Mal am iRMC anmelden

Der iRMC bietet Voreinstellungen, mit denen Sie sich ohne weitere Konfigurationsschritte das erste Mal am iRMC anmelden können.

2.1 Voraussetzungen

Am Remote-Arbeitsplatz:

– Windows: Internet Explorer ab Version 6.x;
Linux: Mozilla Firefox 1.5.

– Für die Konsolumleitung:
Sun Java Virtual Machine 1.5.0_06 oder in einer höheren Version.

In Ihrem Netz:

– Im Ihrem Netz muss sich ein DHCP-Server befinden.

– Wenn Sie sich an der iRMC-Web-Oberfläche an Stelle einer IP-Adresse über einen symbolischen Namen anmelden möchten, muss der DHCP-Server in Ihrem Netz für dynamischen DNS konfiguriert sein.

– DNS muss konfiguriert sein. Andernfalls müssen Sie die IP-Adresse erfragen.

2.2 iRMC-Voreinstellungen

Die Firmware des iRMC stellt eine Standard-Administratorkennung und einen Standard-DHCP-Namen für den iRMC zur Verfügung.

Standard-Administratorkennung:

Administratorkennung: admin

Passwort: admin

Für Administratorkennung und Passwort wird zwischen Groß- und Kleinschreibung unterschieden.

Es wird dringend empfohlen, nach der Anmeldung aus Sicherheitsgründen eine neue Administratorkennung anzulegen und die Standard-Administratorkennung zu löschen oder zumindest das Passwort der Kennung zu ändern (siehe Abschnitt „User Management - Benutzerverwaltung“ auf Seite 263).

Standard-DHCP-Name für den iRMC

Der Standard-DHCP-Name für den iRMC folgt dem Muster:
IRMC<Seriennummer>

Die Seriennummer entspricht den letzten 3 Bytes der MAC-Adresse des iRMC. Die MAC-Adresse des iRMC können Sie dem Aufkleber auf Ihrem PRIMERGY Server entnehmen.

Nach dem Anmelden finden Sie die MAC-Adresse des iRMC als unveränderlichen Eintrag oberhalb der Eingabefelder in der Seite *Network Interface* (siehe Seite 240).

2.3 An der iRMC-Web-Oberfläche anmelden

► Öffnen Sie am Remote-Arbeitsplatz einen Web-Browser und geben Sie den DNS-Namen oder die IP-Adresse des iRMC ein.

Den DNS-Namen des iRMC können Sie dem Aufkleber auf Ihrem PRIMERGY Server entnehmen.

Es wird dann der folgende Anmeldebildschirm angezeigt:

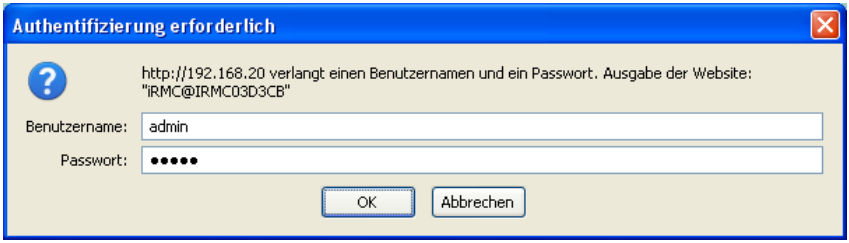


Bild 6: Anmeldebildschirm der iRMC-Web-Oberfläche

Falls der Anmeldebildschirm nicht angezeigt wird, überprüfen Sie die LAN-Verbindung (siehe Abschnitt „LAN-Schnittstelle testen“ auf Seite 43).

► Geben Sie die Daten der Standard-Administratorkennung ein:

Benutzername: admin

Passwort: admin

► Um zu bestätigen, klicken Sie auf die Schaltfläche *OK*.

Die iRMC-Web-Oberfläche öffnet sich, die Seite *System Information (*siehe Seite 190) wird angezeigt.

3 iRMC konfigurieren

Für die Konfiguration des iRMC stehen folgende Tools zur Verfügung:

– BIOS Setup Utility (siehe Seite 41)

– iRMC-Web-Oberfläche (siehe Seite 181)

– Server Configuration Manager (siehe Seite 333)

– Server Management Tool (IPMIVIEW)

Dieses Kapitel informiert über folgende Themen:

– LAN-Schnittstelle des iRMC über das BIOS Setup konfigurieren (siehe Seite 41).

– Text-Konsolumleitung via LAN über das BIOS Setup konfigurieren (siehe Seite 44).

– Serielle Schnittstelle des iRMC über das BIOS Setup konfigurieren (siehe Seite 50).

– iRMC über die Web-Oberfläche konfigurieren (Überblick, siehe Seite 54).

– iRMC über den Server Configuration Manager konfigurieren (Überblick, siehe Seite 56).

3.1 LAN-Schnittstelle des iRMC konfigurieren

Dieser Abschnitt beschreibt:

– Voraussetzungen für die Konfiguration der LAN-Schnittstelle.

– LAN-Schnittstelle im BIOS Setup konfigurieren.

– LAN-Schnittstelle testen.

Für den Switch-Port zum Anschluss des iRMC muss „Spanning Tree“ deaktiviert sein (z.B. Port Fast=enabled; Fast Forwarding=enabled).

3.1.1 Voraussetzungen

Beachten Sie folgende Voraussetzungen für das Konfigurieren der IP-Adresse:

– Die LAN-Verbindung muss am richtigen Port gesteckt sein (siehe Abschnitt „An der richtigen LAN-Schnittstelle gesteckt?“ auf Seite 39).

– Zusammenspiel der IP-Adressen des iRMC und des Systems (siehe Abschnitt „Zusammenspiel der IP-Adressen des iRMC und des Systems“ auf Seite 40).

3.1.1.1 An der richtigen LAN-Schnittstelle gesteckt?

Die Schnittstelle für eine LAN-Verbindung wird bereitgestellt über einen onboard LAN-Controller, der dem iRMC zugeordnet ist (vergleiche Bild 4 auf Seite 28).

Die Systembaugruppe eines PRIMERGY Servers stellt je nach Typ des Servers zwei oder drei LAN-Schnittstellen zur Verfügung. Dem iRMC zugeordnet sind die Ports, die mit dem Symbol eines Schraubenschlüssels gekennzeichnet sind (in Bild 7 ist dies z.B. Port 1).

Prüfen Sie, ob die LAN-Verbindung am richtigen Port gesteckt ist!

Je nach Typ des PRIMERGY Servers können unterschiedliche Ports mit dem Schraubenschlüssel-Symbol gekennzeichnet sein.

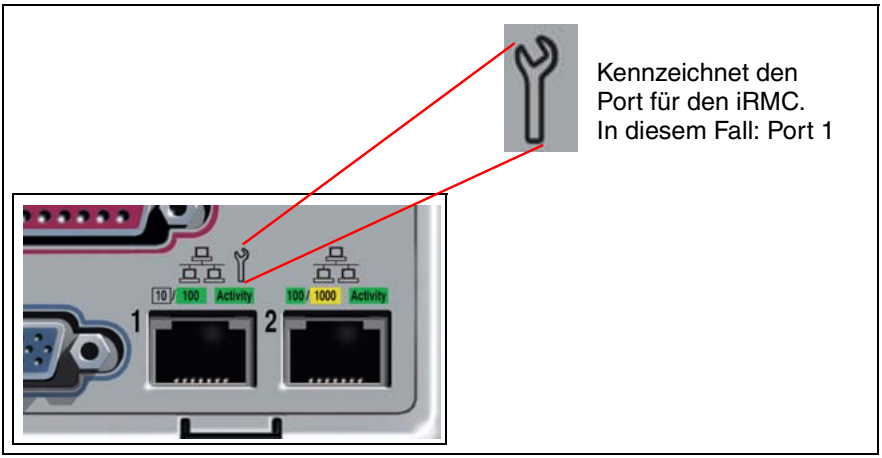


Bild 7: Port für den iRMC (mit Schraubenschlüssel-Symbol gekennzeichnet)

3.1.1.2 Zusammenspiel der IP-Adressen des iRMC und des Systems

Der LAN-Controller des PRIMERGY Servers verlangt eine eigene IP-Adresse für den iRMC, um eine sichere Zustellung von Datenpaketen an den iRMC (und nicht an das Betriebssystem) zu gewährleisten.

Die IP-Adresse des iRMC muss sich von der des Systems (Betriebssystems) unterscheiden.

3.1.1.3 Zugriff aus einem anderen Sub-Netz

Wenn der Remote-Arbeitsplatz aus einem anderen Sub-Netz auf den iRMC des verwalteten Servers zugreift und kein DHCP verwendet wird, müssen Sie das Gateway konfigurieren.

3.1.2 LAN-Schnittstelle konfigurieren: Konfigurationstools

Die LAN-Schnittstelle des iRMC konfigurieren Sie wahlweise je nach Typ des PRIMERGY Servers

- über das BIOS Setup (siehe Seite 41),
- über die iRMC-Web-Oberfläche (siehe Abschnitt „Network Settings - LAN-Parameter konfigurieren“ auf Seite 239),
- über den Server Configuration Manager (siehe „iRMC LAN Interface - LAN-Einstellungen des iRMC konfigurieren“ auf Seite 346),
- über das Server Management Tool (IPMIVIEW).

3.1.3 LAN-Schnittstelle über das BIOS Setup konfigurieren

► Rufen Sie das BIOS-Setup des verwalteten Servers auf.

Drücken Sie während des Boot des Servers die Taste F2.

► Rufen Sie das Menü für die Konfiguration der Peripherie auf:

Advanced – Peripheral Configuration.

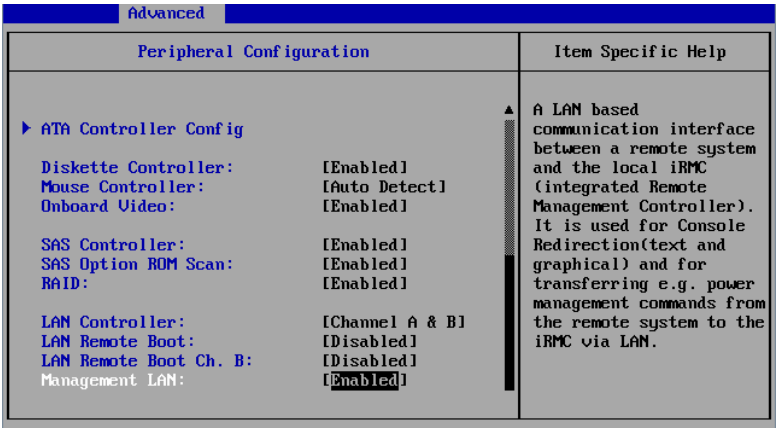

Advanced
Peripheral Configuration
Item Specific Help
ATA Controller Config
Diskette Controller: [Enabled]
Mouse Controller: [Auto Detect]
Onboard Video: [Enabled]
SAS Controller: [Enabled]
SAS Option ROM Scan: [Enabled]
RAID: [Enabled]
LAN Controller: [Channel A & B]
LAN Remote Boot: [Disabled]
LAN Remote Boot Ch. B: [Disabled]
Management LAN: [Enabled]
A LAN based communication interface between a remote system and the local iRMC (integrated Remote Management Controller). It is used for Console Redirection(text and graphical) and for transferring e.g. power management commands from the remote system to the iRMC via LAN.

Bild 8: Menü Peripheral Configuration im BIOS-Setup

► Konfigurieren Sie folgende Einstellung:

Management LAN

Setzen Sie die Einstellung auf *Enabled*.

► Rufen Sie das Menü *LAN-Settings* auf:

Advanced – IPMI – LAN Settings

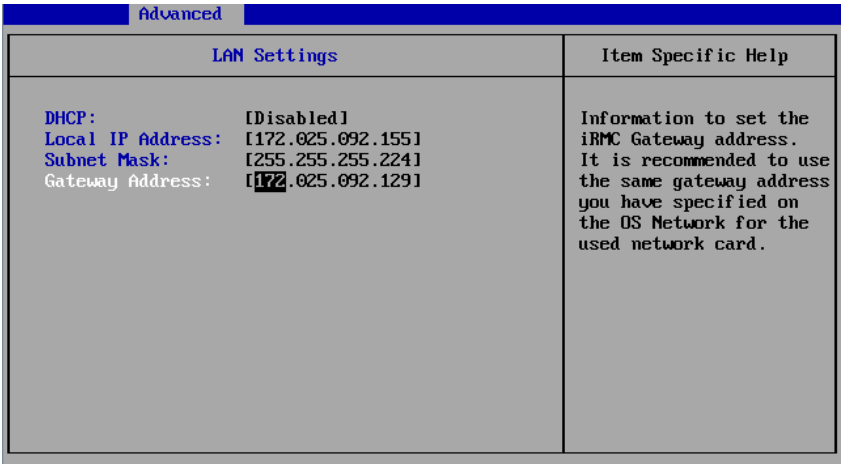

Advanced
LAN Settings
Item Specific Help
DHCP: [Disabled]
Local IP Address: [172.025.092.155]
Subnet Mask: [255.255.255.224]
Gateway Address: [172.025.092.129]
Information to set the iRMC Gateway address. It is recommended to use the same gateway address you have specified on the OS Network for the used network card.

Bild 9: Menü LAN-Settings im BIOS-Setup

► Konfigurieren Sie folgende Einstellungen:

DHCP

Wenn Sie DHCP aktivieren, erfragt der iRMC eigenständig seine LAN-Einstellungen bei einem DHCP-Server im Netzwerk. In diesem Fall werden die Werte *Local IP Address*, *Subnet Mask* usw. automatisch gesetzt.

Aktivieren Sie DHCP nicht, wenn kein DHCP-Server verfügbar ist. Wenn Sie DHCP aktivieren und es ist kein DHCP-Server verfügbar, läuft der iRMC in eine Suchschleife (d.h. er sucht endlos nach einem DHCP-Server).

Die Nutzung der Dienste DHCP und DNS können Sie nach der Erstinstallation z.B. über die iRMC-Web-Oberfläche konfigurieren (siehe Abschnitte „DHCP Configuration - Host-Namen für den iRMC konfigurieren“ auf Seite 247 und „DNS Configuration - DNS für den iRMC aktivieren“ auf Seite 249). Standardmäßig wird bei der Erstinstallation für den iRMC folgende Bezeichnung an den DHCP-Server weitergegeben: *iRMC<letzte 3Bytes der MAC-Adresse>*.

Local IP Address
Geben Sie die recherchierte IP-Adresse für den iRMC des verwalteten Systems an.

Subnet Mask
Geben Sie die Subnet-Maske des Netzwerks an.

Gateway Address
Geben Sie hier die IP-Adresse des Gateways an.

- Sichern Sie die Einstellungen.
- Wenn Sie die Konsolumleitung über den iRMC nutzen möchten, fahren Sie fort mit Abschnitt „Text-Konsolumleitung via LAN über das BIOS Setup konfigurieren“ auf Seite 44.

  Wenn Sie die Text-Konsolumleitung über den iRMC nicht nutzen möchten, beenden Sie das BIOS und fahren Sie fort mit dem nachfolgenden Abschnitt „LAN-Schnittstelle testen“.

3.1.4 LAN-Schnittstelle testen

Für LAN-Schnittstelle können Sie wie folgt testen:

- Versuchen Sie sich über einen Web-Browser an der iRMC-Web-Oberfläche anzumelden. Falls Sie keine Anmeldungsaufforderung erhalten, funktioniert die LAN-Schnittstelle wahrscheinlich nicht.
- Testen Sie die Verbindung zum iRMC mit einem Ping-Kommando.

3.2 Text-Konsolumleitung via LAN über das BIOS Setup konfigurieren

Je nach Konfiguration der Text-Konsolumleitung und Betriebssystem des Servers steht die Text-Konsolumleitung zur Verfügung

– nur für die Dauer der BIOS POST-Phase oder
– über die BIOS POST-Phase hinaus auch bei laufendem Betriebssystem.

Dieser Abschnitt beschreibt:

– Konfiguration der Text-Konsolumleitung via LAN über das BIOS bzw. TrustedCore Setup Utility.

– Betriebssystem-spezifische Besonderheiten, die Sie beachten müssen, wenn Sie die Konsolumleitung auch bei laufendem Betriebssystem nutzen wollen.

Die Text-Konsolumleitung via LAN können Sie auch über die iRMC-Web-Oberfläche konfigurieren (siehe Abschnitt „BIOS Text Console - Text-Konsolumleitung konfigurieren und starten“ auf Seite 281).

3.2.1 Text-Konsolumleitung konfigurieren

► Rufen Sie das BIOS Setup des verwalteten Servers auf. Drücken Sie hierfür während des Boot des Servers die Taste F2.

Einstellungen im Menü für die Konfiguration der Peripherie

► Rufen Sie das Menü für die Konfiguration der Peripherie auf:

Advanced – Peripheral Configuration

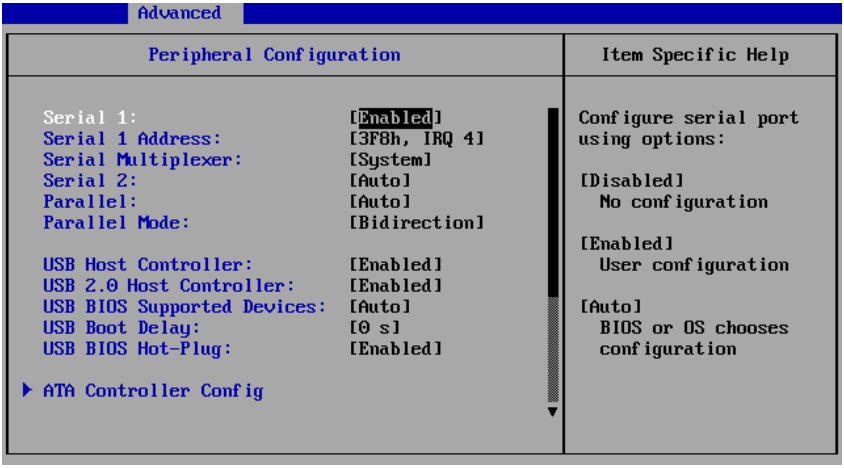


Bild 10: Menü Peripheral Configuration im BIOS Setup

► Konfigurieren Sie folgende Einstellung:

Serial 1
Setzen Sie die Einstellung auf *Enabled*.

Serial 1 Address
Akzeptieren Sie das als erstes vorgeschlagene Wertepaar.

Serial Multiplexer
Setzen Sie die Einstellung auf *System*.

Einstellungen im Menü Console Redirection

- Rufen Sie das Menü *Console Redirection* auf:

  Server – Console Redirection

- Konfigurieren Sie folgende Einstellungen:

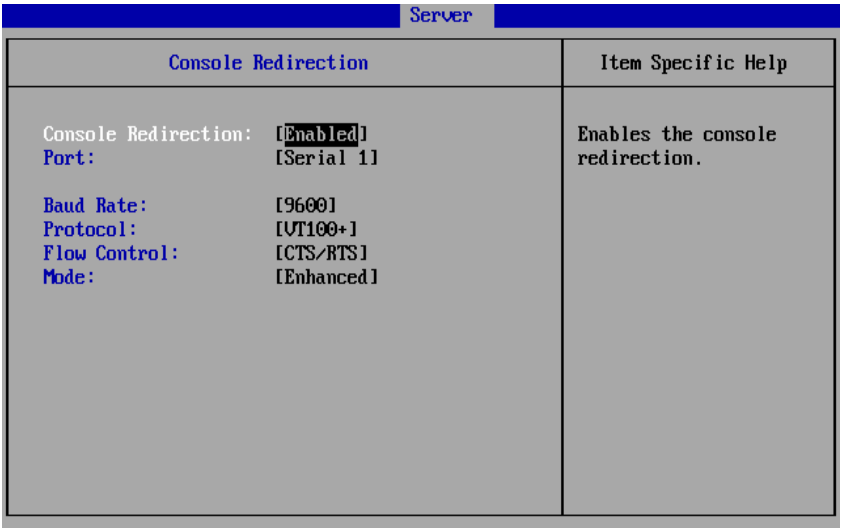


Bild 11: Menü Console Redirection im BIOS Setup

Console Redirection
: Setzen Sie die Einstellung auf *Enabled.*

Port
: Setzen Sie die Einstellung auf *Serial 1*.

Baud Rate
: Legen Sie die Baud-Rate fest.

Protocol
: Lassen Sie diese Einstellung unverändert.(Die Einstellung hängt vom verwendeten Terminal-Typ ab.)

Flow Control
: Lassen Sie diese Einstellung unverändert. (Die Einstellung hängt vom verwendeten Teminal-Typ ab.)

Mode

Diese Einstellung wirkt sich auf das Verhalten der Konsolumleitung bei laufendem Betriebssystem (nach der POST-Phase) aus (siehe Abschnitt „Konsolumleitung bei laufendem Betriebssystem nutzen“ auf Seite 48):

Standard

Die Konsolumleitung wird nach der POST-Phase des BIOS beendet.

Enhanced

Die Konsolumleitung steht über die POST-Phase des BIOS hinaus zur Verfügung.

BIOS Setup beenden

- Sichern Sie die Einstellungen und beenden Sie das BIOS Setup.
- Fahren Sie fort mit Abschnitt „LAN-Schnittstelle testen“ auf Seite 43.

3.2.2 Konsolumleitung bei laufendem Betriebssystem nutzen

Sie können - je nach Betriebssystem des verwalteten Servers - auch nach der BIOS POST-Phase noch die Konsolumleitung nutzen.

DOS

Die BIOS-Einstellung für den Modus der Konsolumleitung muss wie folgt konfiguriert sein (siehe Abschnitt „Einstellungen im Menü Console Redirection“ auf Seite 46):

– BIOS Setup Utility: *Mode: Enhanced*

– TrustedCore Setup Utility: *Continue C.R. after POST: On*

Windows Server 2003

Windows Server 2003 übernimmt nach der POST-Phase automatisch die Konsolumleitung, ohne dass weitere Einstellungen notwendig sind. Während der Boot-Phase des Betriebssystems wird die SAC-Konsole von Windows Server 2003 übertragen:

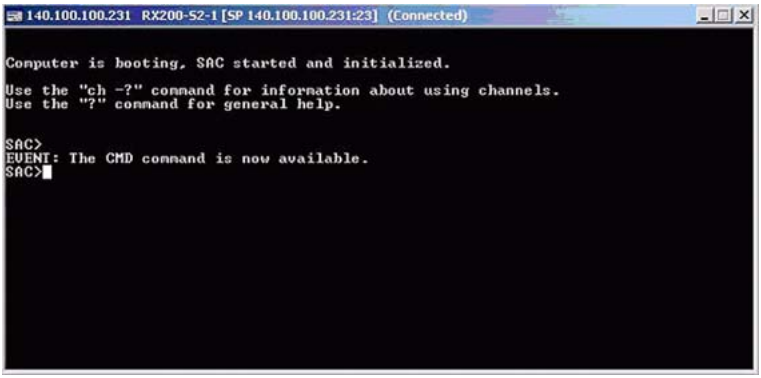

140.100.100.231 RX200-S2-1 [SP 140.100.100.231:23] (Connected)
Computer is booting, SAC started and initialized.
Use the "ch -?" command for information about using channels.
Use the "?" command for general help.
SAC>
EVENT: The CMD command is now available.
SAC>

Bild 12: SAC-Konsole von Windows Server 2003

Linux

Ein Linux-Betriebssystem müssen Sie konfigurieren, damit es die Konsolumleitung nach der POST-Phase übernimmt. Wenn es konfiguriert ist, haben Sie vom Remote-Arbeitplatz aus vollen Zugriff.

Notwendige Einstellungen

Die Einstellungen können sich je nach Programmversion etwas ändern.

SuSe und RedHat

Fügen Sie am Ende der Datei */etc/inittab* folgende Zeile an:

```
xx:12345:respawn:/sbin/agetty <baudrate> ttyS0
```

RedHat

Fügen Sie in die Datei */etc/grub.conf* folgenden Kernel-Boot-Parameter ein:

```
console=ttyS0,<baudrate> console=tty0
```

SuSE

Fügen Sie in die Datei */boot/grub/menu.lst* folgenden Kernel-Boot-Parameter ein:

```
console=ttyS0,<baudrate> console=tty0
```

3.3 Die serielle Schnittstelle des iRMC konfigurieren und nutzen

Die serielle Schnittstelle des iRMC bietet Ihnen folgende Möglichkeiten:

– Über Nullmodem-Kabel können Sie die Terminal-Anwendung Remote Manager (Serial) nutzen (siehe Abschnitt „Benutzeroberfläche Remote Manager (Serial) nutzen“ auf Seite 53).

– Weiterleitung von Alarmen über Modem (Alerting). Das Alerting via Modem können Sie über die Web-Oberfläche des iRMC konfigurieren (siehe Abschnitt „Serial / Modem Alerting - Alarmweiterleitung über Modem konfigurieren“ auf Seite 254).

3.3.1 Die serielle Schnittstelle konfigurieren

Einstellungen im BIOS

- Rufen Sie das BIOS Setup des verwalteten Servers auf. Drücken Sie hierfür während des Boot des Servers die Taste F2.
- Rufen Sie das Menü *Peripheral Configuration* auf, um den seriellen Port zu konfigurieren:

  Advanced – Peripheral Configuration

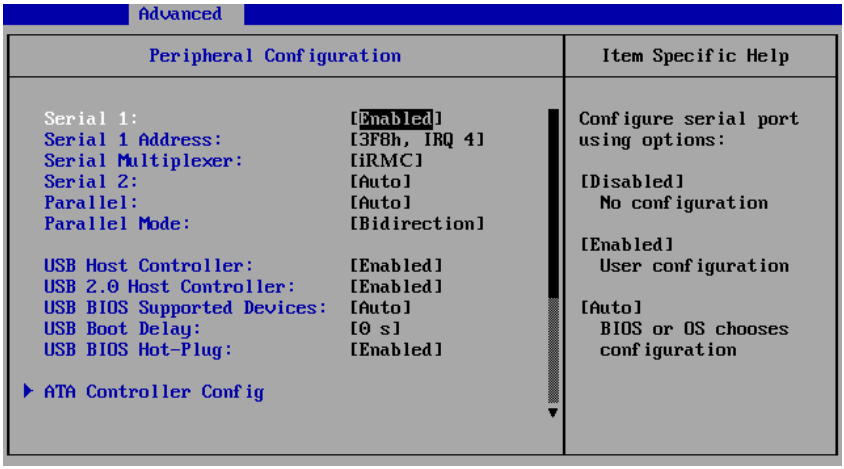


Bild 13: Menü Peripheral Configuration

- Konfigurieren Sie folgende Einstellung:

  Serial 1
  Setzen Sie die Einstellung auf *Enabled*.

  Serial 1 Address
  Akzeptieren Sie das als erstes vorgeschlagene Wertepaar.

  Serial Multiplexer
  Setzen Sie die Einstellung auf *iRMC*.

Die folgenden, im Menü nicht angezeigten Werte sind voreingestellt (siehe Seite 53, "Terminalprogramm (VT100+)"):

Bits per second
9600

Data bits
8

Parity
None.

Stop bits
1

Flow Control
None

BIOS / TrustedCore Setup beenden

- Sichern Sie die Einstellungen und beenden Sie das BIOS bzw. TrustedCore Setup Utility.
- Fahren Sie fort mit Abschnitt „LAN-Schnittstelle testen“ auf Seite 43.

3.3.2 Benutzeroberfläche Remote Manager (Serial) nutzen

Wenn Sie über eine Nullmodemkabel einen Rechner anschließen und auf diesem Rechner ein Terminalprogramm (VT100+) starten, können Sie auf die Terminal-Anwendung Remote Manager (Serial) zugreifen. Die Oberfläche des Remote Manager (Serial) ist identisch mit der Oberfläche des Remote Manager (siehe Kapitel „iRMC über Telnet/SSH (Remote Manager) bedienen“ auf Seite 307).

Voraussetzungen

Am verwalteten Server:

Die BIOS-Einstellung *Serial Multiplexer* muss auf *iRMC* konfiguriert sein (siehe Abschnitt „Die serielle Schnittstelle konfigurieren“ auf Seite 51).

Terminalprogramm (VT100+):

Konfigurieren Sie für das Terminalprogramm folgende Port-Einstellungen:

Bits per second

Setzen Sie die Einstellung auf *9600*.

Data bits

Setzen Sie die Einstellung auf *8*.

Parity

Setzen Sie die Einstellung auf *None*.

Stop bits

Setzen Sie die Einstellung auf *1*.

Flow Control

Setzen Sie die Einstellung auf *None*.

3.4 iRMC über die iRMC-Web-Oberfläche konfigurieren

► Starten Sie die iRMC-Web-Oberfläche (siehe Abschnitt „An der iRMC-Web-Oberfläche anmelden“ auf Seite 182).

3.4.1 LAN-Parameter konfigurieren

► Wählen Sie im Navigationsbereich den Eintrag *Network Settings* (siehe Abschnitt „Network Settings - LAN-Parameter konfigurieren“ auf Seite 239).

LAN-Einstellungen konfigurieren

► Konfigurieren Sie die LAN-Einstellungen in der Seite *Network Interface*. Für die erforderlichen Einstellungen siehe Abschnitt „Network Interface - Ethernet-Einstellungen des iRMC konfigurieren“ auf Seite 240.

Ports und Netzdienste konfigurieren

► Konfigurieren Sie die Ports und Netzdienste in der Seite *Ports und Network Services*. Für die erforderlichen Einstellungen siehe Abschnitt „Ports and Network Services - Ports und Netzdienste konfigurieren“ auf Seite 243.

DHCP konfigurieren

► Konfigurieren Sie die DHCP-Einstellungen in der Seite *DHCP Configuration*. Für die erforderlichen Einstellungen siehe Abschnitt „DHCP Configuration - Host-Namen für den iRMC konfigurieren“ auf Seite 247.

DNS konfigurieren

► Konfigurieren Sie die DNS-Einstellungen in der Seite *DNS Settings*. Für die erforderlichen Einstellungen siehe Abschnitt „DNS Configuration - DNS für den iRMC aktivieren“ auf Seite 249.

3.4.2 Alarmbenachrichtigung (Alerting) konfigurieren

Die Seiten für die Konfiguration der Alarmbenachrichtigung sind im Navigationsbereich unter „Alerting“ zusammengefasst (siehe Abschnitt „Alerting - Alarmbenachrichtigung konfigurieren“ auf Seite 251).

Weiterleitung von Alarmen über SNMP konfigurieren

- Klicken Sie im Navigationsbereich auf *SNMP Traps*. Die Seite *SNMP Traps* wird angezeigt.
- Konfigurieren Sie die Weiterleitung von SNMP Traps. Für die erforderlichen Einstellungen siehe Abschnitt „SNMP Trap Alerting - SNMP-Alarmweiterleitung konfigurieren“ auf Seite 252.

Weiterleitung von Alarmen über Modem an Mobiltelefon konfigurieren

- Klicken Sie im Navigationsbereich auf *Serial / Modem*. Die Seite *Serial Modem Alerting* wird angezeigt.
- Konfigurieren Sie die Weiterleitung von Alarmen über Modem. Für die erforderlichen Einstellungen siehe Abschnitt „Serial / Modem Alerting - Alarmweiterleitung über Modem konfigurieren“ auf Seite 254.

E-Mail-Benachrichtigung (Email Alerting) konfigurieren

- Klicken Sie im Navigationsbereich auf *Email*. Die Seite *Email Alerting* wird angezeigt.
- Konfigurieren Sie die E-Mail-Benachrichtigung. Für die erforderlichen Einstellungen siehe Abschnitt „Email Alerting - E-Mail-Benachrichtigung konfigurieren“ auf Seite 256.

3.4.3 Text-Konsolumleitung konfigurieren

- Konfigurieren Sie die Umleitung der Text-Konsole im Fenster *BIOS Text Console*. Für die erforderlichen Einstellungen siehe Abschnitt „BIOS Text Console - Text-Konsolumleitung konfigurieren und starten“ auf Seite 281.

3.5 iRMC über den Server Configuration Manager konfigurieren

► Starten Sie den Server Configuration Manager (siehe Kapitel „iRMC via Server Configuration Manager konfigurieren“ auf Seite 333).

3.5.1 LAN-Parameter konfigurieren

LAN-Einstellungen konfigurieren

► Konfigurieren Sie die LAN-Einstellungen im Dialog *iRMC LAN Interface*. Für die erforderlichen Einstellungen siehe Abschnitt „iRMC LAN Interface - LAN-Einstellungen des iRMC konfigurieren“ auf Seite 346.

Ports und Netzdienste konfigurieren

► Konfigurieren Sie die Ports und Netzdienste im Dialog *iRMC Networking Ports*. Für die erforderlichen Einstellungen siehe Abschnitt „iRMC Networking Ports - Ports und Netzdienste konfigurieren“ auf Seite 349.

DHCP/DNS („Dynamic DNS“) konfigurieren

► Konfigurieren Sie die DHCP-Einstellungen im Dialog *iRMC DNS Registration*. Für die erforderlichen Einstellungen siehe Abschnitt „iRMC DNS Registration - Host-Namen für den iRMC konfigurieren“ auf Seite 351.

DNS konfigurieren

► Konfigurieren Sie die DNS-Einstellungen im Dialog *iRMC DNS Server*. Für die erforderlichen Einstellungen siehe Abschnitt „iRMC DNS Server - DNS für den iRMC aktivieren“ auf Seite 353.

3.5.2 Alarmbenachrichtigung (Alerting) konfigurieren

Weiterleitung von Alarmen über SNMP konfigurieren

- Konfigurieren Sie die Weiterleitung von SNMP Traps im Dialog *iRMC SNMP Alerting*. Für die erforderlichen Einstellungen siehe Abschnitt „iRMC SNMP Alerting - SNMP-Alarm-Weiterleitung konfigurieren“ auf Seite 360.

E-Mail-Benachrichtigung (Email Alerting) konfigurieren

- Konfigurieren Sie die globalen E-Mail-Einstellungen im Dialog *iRMC EMail Alerting*. Für die erforderlichen Einstellungen siehe Abschnitt „iRMC EMail Alerting - E-Mail-Weiterleitung konfigurieren“ auf Seite 355.
- Konfigurieren Sie die Benutzer-spezifischen E-Mail-Einstellungen im Dialog *iRMC EMail Format Settings*. Für die erforderlichen Einstellungen siehe Abschnitt „iRMC Mail Format Settings - Mail-Format-abhängige Einstellungen“ auf Seite 358.

4 Benutzerverwaltung für den iRMC

Die Benutzerverwaltung für den iRMC verwendet zwei verschiedene Arten von Benutzerkennungen:

– Lokale Benutzerkennungen sind lokal im nicht-flüchtigen Speicher des iRMC hinterlegt und werden über die Benutzerschnittstellen des iRMC verwaltet.

– Globale Benutzerkennungen sind in der zentralen Datenhaltung eines Directory Service hinterlegt und werden über die Schnittstellen dieses Directory Service verwaltet.

  Für die globale iRMC-Benutzerverwaltung werden zurzeit folgende Directory Services unterstützt:

  – Microsoft® Active Directory
  – Novell® eDirectory
  – OpenLDAP

Das vorliegende Kapitel informiert über folgende Themen:

– Konzept der Benutzerverwaltung für den iRMC
– Benutzerberechtigungen
– lokale Benutzerverwaltung am iRMC
– globale Benutzerverwaltung mithilfe der einzelnen Directory Services

4.1 Konzept der Benutzerverwaltung für den iRMC

Die Benutzerverwaltung für den iRMC unterstützt die parallele Verwaltung lokaler und globaler Benutzerkennungen.

Bei der Validierung der Authentisierungsdaten (Benutzername, Passwort), die ein Benutzer beim Login an einer der iRMC-Schnittstellen eingibt, verfährt der iRMC gemäß dem folgenden Ablauf (siehe auch Bild 14 auf Seite 61):

1. Der iRMC gleicht den Benutzernamen und das Passwort mit den lokal gespeicherten Benutzerkennungen ab:
   - Bei erfolgreicher Authentisierung des Benutzers (Benutzername und Passwort sind gültig) darf sich der Benutzer einloggen.
   - Andernfalls setzt der iRMC die Prüfung mit Schritt 2. fort.
2. Der iRMC authentisiert sich beim Directory Service via LDAP mit Benutzernamen und Passwort, ermittelt per LDAP-Anfrage die Benutzerrechte und prüft, ob der Benutzer damit am iRMC arbeiten darf.

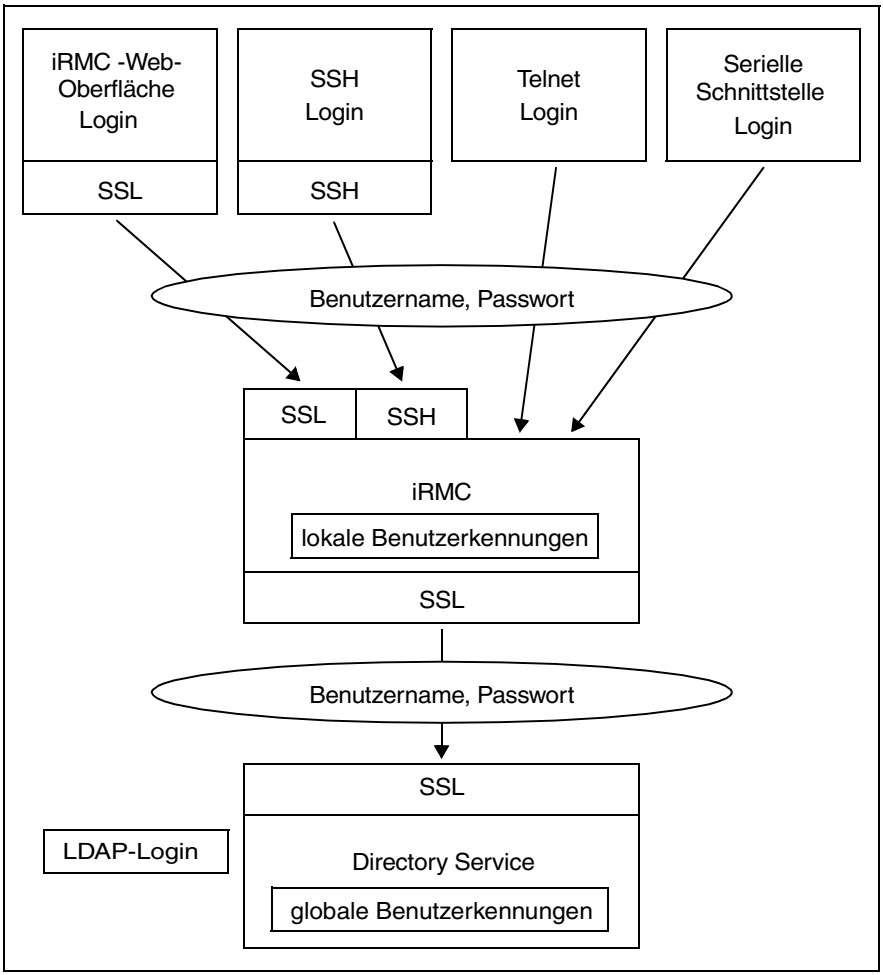


Bild 14: Login-Authentifizierung durch den iRMC

Die Nutzung von SSL für die LDAP-Verbindung zwischen dem iRMC und dem Directory Service ist optional, wird jedoch empfohlen. Eine SSL-gesicherte LDAP-Verbindung zwischen iRMC und Directory Service garantiert den sicheren Austausch der Daten, insbesondere auch von Benutzernamen und Passwort.

SSL-Login über die iRMC-Web-Oberfläche ist nur dann erforderlich, wenn LDAP aktiviert ist (Option *LDAP enable*, siehe Seite 274).

4.2 Benutzerberechtigungen

Der iRMC unterscheidet zwei verschiedene Arten von Benutzerberechtigungen, die sich ergänzen:

– Kanal-spezifische Privilegien (via Zuordnung zu Kanal-spezifischen Berechtigungsgruppen)

– Berechtigungen zur Nutzung spezieller iRMC-Funktionen

Welche dieser Privilegien und Berechtigungen zur Nutzung der einzelnen iRMC-Funktionen erforderlich sind, ist beschrieben

– für die iRMC-Web-Oberfläche auf Seite 184,

– für den Remote Manager auf Seite 316,

Kanal-spezifische Privilegien (Kanal-spezifische Berechtigungsgruppen)

Der iRMC ordnet jede Benutzerkennung einer der folgenden vier kanal-spezifischen Berechtigungsgruppen zu:

– User
– Operator
– Administrator
– OEM

Da der iRMC diese Berechtigungen Kanal-spezifisch erteilt, kann ein Benutzer verschiedene Rechte haben, je nachdem, ob er auf den iRMC über die LAN-Schnittstelle oder über die serielle Schnittstelle zugreift.

Der Berechtigungsumfang nimmt beginnend bei *User* (niedrigste Berechtigungsstufe) über *Operator* und *Administrator* bis *OEM* (höchste Berechtigungsstufe) stetig zu.

Die Berechtigungsgruppen entsprechen dem IPMI Privilege Level. Bestimmte Rechte (z. B. für das Power Management) sind an diese Gruppen bzw. Privilege Level gebunden.

Berechtigungen zur Nutzung spezieller iRMC-Funktionen

Zusätzlich zu den Kanal-spezifischen Berechtigungen können Sie einem Benutzer individuell folgende Berechtigungen erteilen:

- **Configure User Accounts**
  Berechtigung zum Konfigurieren von lokalen Benutzerkennungen
- **Configure iRMC Settings**
  Berechtigung zum Konfigurieren der iRMC-Einstellungen
- **Video Redirection Enabled**
  Berechtigung zur Nutzung der Advanced Video Redirection (AVR) im „View Only“- und „Full Control“- Modus
- **Remote Storage Enabled**
  Berechtigung zur Nutzung der Remote Storage-Funktionalität

Vorkonfigurierte Benutzerkennung

Die Firmware des iRMC stellt eine Standard-Administratorkennung für den iRMC zur Verfügung, die sämtliche Berechtigungen besitzt:

Administratorkennung: admin

Passwort: admin

Für Administratorkennung und Passwort wird bei lokalen Benutzern zwischen Groß- und Kleinschreibung unterschieden.

Es wird dringend empfohlen, nach der Anmeldung möglichst bald eine neue Administratorkennung anzulegen und die Standard-Administratorkennung zu löschen oder zumindest das Passwort der Kennung zu ändern (siehe Abschnitt „User Management - Benutzerverwaltung“ auf Seite 263).

4.3 Lokale Benutzerverwaltung für den iRMC

Der iRMC verfügt über eine eigene lokale Benutzerverwaltung. Es können bis zu 16 Benutzer mit Passwörtern konfiguriert und je nach Gruppenzugehörigkeit mit unterschiedlichen Rechten ausgestattet werden. Die Benutzerkennungen werden im lokalen, nicht-flüchtigen Speicher des iRMC abgelegt. Die Benutzerverwaltung können Sie manuell oder Skript-basiert (mit IPMIView) durchführen.

Für die Benutzerverwaltung am iRMC stehen Ihnen folgende Möglichkeiten zur Verfügung:

– Benutzerverwaltung über die Web-Oberfläche
– Benutzerverwaltung über den Server Configuration Manager
– Benutzerverwaltung über das Server Management Tool (IPMIVIEW)

4.3.1 Lokale Benutzerverwaltung über die iRMC-Web-Oberfläche

Die Benutzerverwaltung am iRMC erfordert *Configure User Accounts*-Berechtigung.

An der Web-Schnittstelle können Sie sich die Liste der konfigurierten Benutzer anzeigen lassen. Außerdem können Sie neue Benutzer konfigurieren, die Konfiguration bereits existierender Benutzer ändern sowie Benutzer aus der Liste entfernen.

► Starten Sie die iRMC-Web-Oberfläche (siehe Abschnitt „An der iRMC-Web-Oberfläche anmelden“ auf Seite 182).

Liste der konfigurierten Benutzer anzeigen

► Klicken Sie im Navigationsbereich auf den die Funktion *iRMC User*.

Die Seite *User Management* mit der Liste der konfigurierten Benutzer öffnet sich (siehe Seite 264). Dort können Sie Benutzer löschen sowie die Seite für die Konfiguration neuer Benutzer aufrufen.
Die Beschreibung zu dieser Seite finden Sie im Abschnitt „User Management - Benutzerverwaltung“ auf Seite 263.

Neuen Benutzer konfigurieren

► Klicken Sie in der Seite *User Management* auf die Schaltfläche *New User*.

Die Seite *New User Configuration* öffnet sich. In dieser Seite können Sie die Grundeinstellungen des neuen Benutzers spezifizieren. Die Beschreibung zu dieser Seite finden Sie im Abschnitt „New User Configuration - Neuen Benutzer konfigurieren“ auf Seite 265.

Konfiguration eines Benutzers ändern

► Klicken Sie in der Seite *User Management* auf den Namen des Benutzers, dessen Konfigurationsparameter Sie ändern wollen.

Die Seite *User "<name>" Configuration* öffnet sich mit den Einstellungen des ausgewählten Benutzers. Dort können Sie die Konfigurationsparameter des neuen Benutzers modifizieren. Die Beschreibung zu dieser Seite finden Sie im Abschnitt „User ’<name>’ Configuration - Benutzerkonfiguration (Details)“ auf Seite 266.

Benutzer löschen

► Klicken Sie in der Seite *User Management* auf die Schaltfläche *Delete*, die sich in der Zeile des zu löschenden Benutzers befindet.

4.3.2 Lokale Benutzerverwaltung über den Server Configuration Manager

Voraussetzung:

Auf dem verwalteten Server sind die aktuellen ServerView-Agenten installiert.

Die Benutzerverwaltung am iRMC erfordert *Configure User Accounts*-Berechtigung.

Über den Server Configuration Manager können Sie sich die Liste der konfigurierten Benutzer anzeigen lassen. Außerdem können Sie neue Benutzer konfigurieren, die Konfiguration bereits existierender Benutzer ändern sowie Benutzer aus der Liste entfernen.

- Starten Sie den Server Configuration Manager (siehe Kapitel „iRMC via Server Configuration Manager konfigurieren“ auf Seite 333).

Liste der konfigurierten Benutzer anzeigen

- Wählen Sie den Dialog *iRMC User Management*.

  Der Dialog enthält eine Liste aller konfigurierten Benutzer (siehe Seite 361). Dort können Sie Benutzer löschen sowie das Fenster *Edit existing user* aufrufen, das die Einstellungen des ausgewählten Benutzers anzeigt. Die Beschreibung zu diesem Fenster finden Sie auf Seite 362.

Neuen Benutzer konfigurieren

- Markieren Sie im Dialog *iRMC User Management* unterhalb der angezeigten Benutzer eine Zeile, in der nur die User ID angezeigt wird.
- Klicken Sie auf die Schaltfläche *Modify...* oder führen Sie einen Doppel-Klick auf die markierte Zeile aus.

  Das Fenster *Edit existing user* öffnet sich.
- Tragen Sie im Fenster *Edit existing user* die Einstellungen für den neuen Benutzer ein.
- Bestätigen Sie Ihre Einstellungen mit *OK*.

Konfiguration eines Benutzers ändern

- ► Markieren Sie im Dialog *iRMC User Management* einen Benutzer.
- ► Klicken Sie auf die Schaltfläche *Modify...* oder führen Sie einen Doppel-Klick auf den markierten Benutzer aus.

  Das Fenster *Edit existing user* mit den konfigurierten Einstellungen für diesen Benutzer öffnet sich.
- ► Modifizieren Sie im Fenster *Edit existing user* die Einstellungen für den Benutzer.
- ► Bestätigen Sie die Einstellungen mit *OK*.

Benutzer löschen

- ► Markieren Sie im Dialog *iRMC User Management* einen Benutzer.
- ► Klicken Sie auf die Schaltfläche *Delete...*, um den Benutzer zu löschen.

4.4 Globale Benutzerverwaltung für den iRMC

Die globalen Benutzerkennungen für den iRMC werden zentral mithilfe eines LDAP Directory Service verwaltet.

Für die iRMC-Benutzerverwaltung werden zurzeit folgende Directory Services unterstützt:

– Microsoft® Active Directory
– Novell® eDirectory
– OpenLDAP

Dieser Abschnitt informiert über folgende Themen:

– Überblick über die globale Benutzerverwaltung für den iRMC
– Konzept der globalen Benutzerverwaltung für den iRMC mithilfe eines LDAP Directory Service
– Globale iRMC-Benutzerverwaltung im Directory Service konfigurieren (Struktur *iRMCgroups* im Directory Service generieren).
– Globale iRMC-Benutzerverwaltung via Microsoft Active Directory
– Globale iRMC-Benutzerverwaltung via Novell eDirectory
– Globale iRMC-Benutzerverwaltung via OpenLDAP

Neben den in diesem Abschnitt beschriebenen Maßnahmen, die Sie auf Seiten des Directory Service durchführen, erfordert die globale Benutzerverwaltung außerdem die Konfiguration der lokalen LDAP-Einstellungen am iRMC.

Die lokalen LDAP-Einstellungen konfigurieren Sie wahlweise

– an der iRMC-Web-Oberfläche (siehe Seite Seite 273),
– mithilfe des Server Configuration Manager (siehe Seite Seite 367) oder
– mithilfe des Server Management Tools (IPMIVIEW).

4.4.1 Überblick

Die globalen Benutzerkennungen für den iRMC werden zentral abgelegt im Verzeichnis (Directory) eines Directory Service. Auf diese Weise lassen sich die Benutzerkennungen auf einem zentralen Server verwalten und können somit von allen iRMCs verwendet werden, die mit diesem Server im Netz verbunden sind.

Der Einsatz eines Directory Service für den iRMC ermöglicht es darüber hinaus, für das Login an den iRMCs dieselben Benutzerkennungen zu verwenden wie für das Login am Betriebssystem der verwalteten Server.

Für die folgenden iRMC-Funktionen wird zurzeit die globale Benutzerverwaltung nicht unterstützt:

- Login via IPMI-over-LAN
- Alerting
- Text-Konsolumleitung via SOL

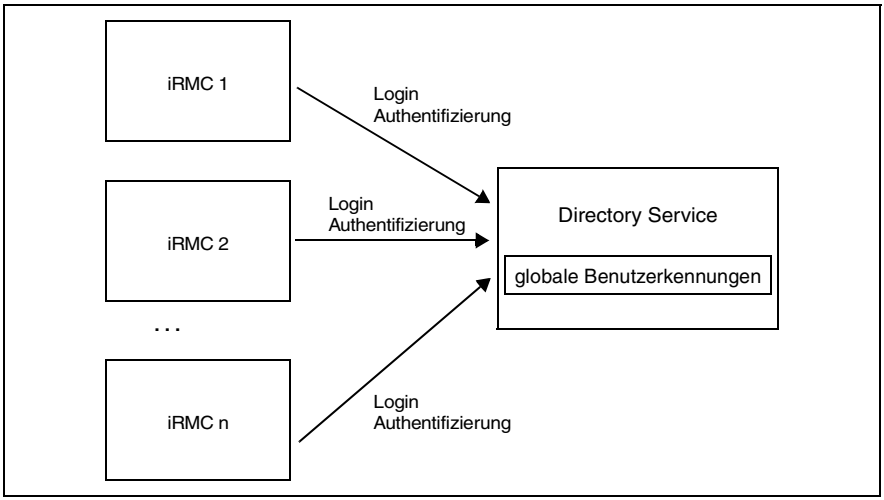


Bild 15: Gemeinsame Nutzung der globalen Benutzerkennungen durch mehrere iRMCs

Die Kommunikation zwischen den einzelnen iRMCs und dem zentralen Directory Service wird über das TCP/IP-Protokoll LDAP (**L**ightweight **D**irectory **A**ccess **P**rotocol) abgewickelt. LDAP ermöglicht den Zugriff auf die gängigsten zur Benutzerverwaltung geeigneten Directory Services. Die Kommunikation über LDAP kann optional durch SSL abgesichert werden.

4.4.2 iRMC-Benutzerverwaltung mithilfe eines LDAP Directory Service (Konzept)

Das im Folgenden erläuterte Konzept einer Directory Service-gestützten, globalen iRMC-Benutzerverwaltung gilt gleichermaßen für die Directory Services Microsoft Active Directory, Novell eDirectory und OpenLDAP. Die Abbildungen zeigen exemplarisch die Konsole *Active Directory-Benutzer und -Computer* der Benutzeroberfläche von Microsoft Active Directory.

Die folgenden Zeichen sind in LDAP als Meta-Zeichen für Such-Strings reserviert: &, |, !, =, <, >, ~, :

Verwenden Sie diese Zeichen deshalb nicht als Bestandteil von Relative Distinguished Names (RDN).

4.4.2.1 Globale Benutzerverwaltung über die OU „iRMCgroups“

Die globale iRMC-Benutzerverwaltung mithilfe eines LDAP Directory Servers erfordert keine Erweiterung des Standard-Schemas des Directory Servers. Vielmehr werden sämtliche für den iRMC relevanten Informationen einschließlich der Privilegien über zusätzliche LDAP-Gruppen und Organizational Units (OU) bereitgestellt, die in einer separaten OU *iRMCgroups* in der Base Domain des LDAP Directory Servers zusammengefasst sind (siehe Bild 16).

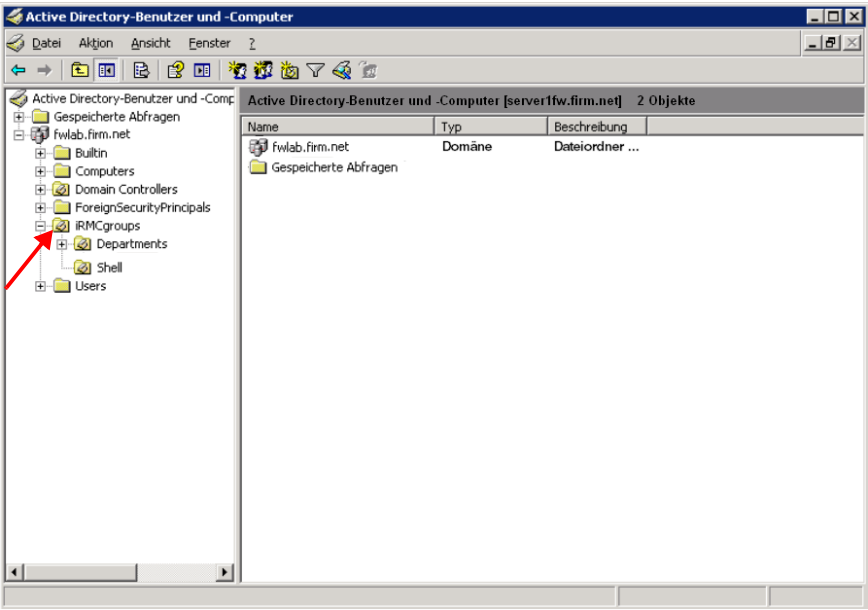


Bild 16: OU iRMCgroups in der Base Domain fwlab.firm.net

Ein iRMC-Benutzer erhält seine Privilegien über die Zugehörigkeit zu einer Gruppe der OU *iRMCgroups*.

Die Benutzereinträge für den iRMC können an beliebigen Stellen unterhalb der Base Domain liegen, in der die OU *iRMCgroups* enthalten ist.

iRMCgroups selbst enthält die OUs *Departments* und *Shell*:

– *Departments* enthält die Gruppen für die Benutzerprivilegien.

– *Shell* enthält die Gruppen für die Benutzershells.

Bei Microsoft Active Directory z.B. können die Einträge für die iRMC-Benutzer in der Standard OU *Users* liegen. Im Gegensatz zu den Standardbenutzern sind iRMC-Benutzer jedoch zusätzlich Mitglied in einer oder mehreren Gruppen der OU *iRMCgroups*.

4.4.2.2 Server-übergreifende globale Benutzerberechtigungen

In größeren Unternehmen sind die via iRMC verwalteten Server in der Regel verschiedenen Abteilungen zugeordnet. Außerdem werden die Administratorberechtigungen für die verwalteten Server ebenfalls oft abteilungsspezifisch vergeben.

Abteilungen sind in der OU „Departments“ zusammengefasst

Die OU *Departments* fasst die via iRMC verwalteten Server zu verschiedenen Gruppen zusammen. Diese entsprechen den Abteilungen, in denen jeweils dieselben Benutzerkennungen und -berechtigungen gelten. In Bild 17 auf Seite 73 z.B. sind dies die Abteilungen *DeptX*, *DeptY* und *Others*.

Der Eintrag *Others* ist optional, wird aber empfohlen. *Others* ist eine vordefinierte Abteilungsbezeichnung, unter der die Server zusammengefasst sind, die keiner anderen Abteilung angehören. Die Anzahl der unter *Departments* aufgelisteten Abteilungen (OUs) unterliegt keinen Einschränkungen.

Bei der Konfiguration des Directory Service am iRMC über die iRMC-Web-Oberfläche (siehe Seite 273), über den Server Configuration Manager (siehe Seite 367) oder das Server Manangement Tool (IPMIVIEW) spezifizieren Sie den Namen der Abteilung, welcher der verwaltete Server mit dem betreffenden iRMC angehört. Existiert im LDAP Directory keine Abteilung dieses Namens, dann werden die Berechtigungen der Abteilung *Others* verwendet.

Bild 17 zeigt anhand von *Active Directory-Benutzer und -Computer* ein Beispiel für eine solche Organisationsstruktur.

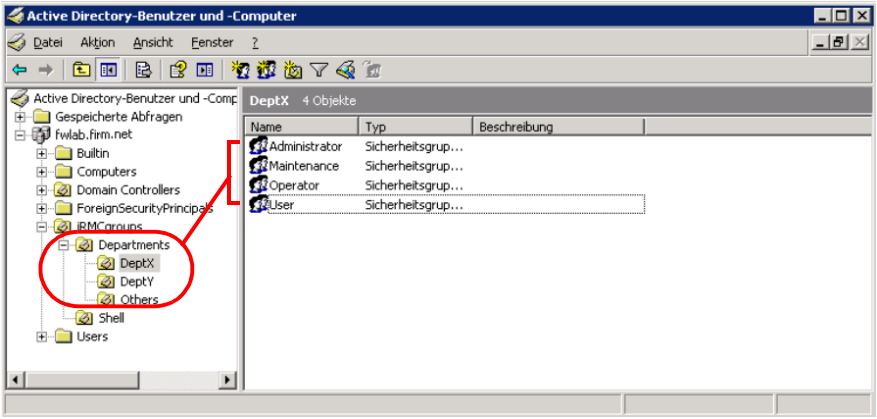


Bild 17: Organistionsstruktur der Domäne fwlab.firm.net

Berechtigungsprofile werden über Berechtigungsgruppen definiert

Direkt unterhalb jeder Abteilung sind die zugehörigen Berechtigungsgruppen (Sicherheitsgruppen) angesiedelt. Hinsichtlich der Anzahl der Berechtigungsgruppen gibt es keine Einschränkungen. Die Namen der Berechtigungsgruppen sind unter Beachtung einiger syntaktischer Vorgaben des verwendeten Directory Service frei wählbar. Jede Berechtigungsgruppe definiert ein spezifisches Berechtigungsprofil, das sich auf alle Benutzer erstreckt, die der betreffenden Berechtigungsgruppe angehören.

ACHTUNG!

Stellen Sie sicher, dass ein Benutzer gleichzeitig nie mehr als einer Berechtigungsgruppe derselben Abteilung angehört. (Gehört ein Benutzer zu mehr als einer Berechtigungsgruppe derselben Abteilung, so ist immer das zuerst gelieferte Ergebnis einer LDAP-Anfrage relevant.)

Die Berechtigungsgruppen der globalen iRMC-Benutzerverwaltung umfassen auch die Kanal-spezifischen Berechtigungsgruppen (siehe Seite 62). Ausführliche Informationen zu den einzelnen Benutzerberechtigungen finden Sie im Abschnitt „Benutzerberechtigungen“ auf Seite 62.

Wenn Sie z.B. im Strukturbaum von *Active Directory-Benutzer und -Computer* (siehe Bild 18) auf eine Abteilung (z.B. *DeptX*) klicken (1), werden im Anzeigebereich die Berechtigungsgruppen (Sicherheitsgruppen) angezeigt, die für diese Abteilung (hier: *DeptX*) definiert sind.

Durch Klicken auf eine der angezeigten Sicherheitsgruppen (2), wird die *Eigenschaften*-Dialogbox dieser Sicherheitsgruppe (hier: *Maintenance*) geöffnet. Unter *Anmerkung:* ist das zugehörige Berechtigungsprofil gemäß der folgenden Syntax aufgelistet:

```
LAN: OEM | Administrator | Operator | User | None
Serial: OEM | Administrator | Operator | User | None
UserAccounts: On | Off
iRMCsettings: On | Off
Video Redirection: On | Off
Remote Storage: On | Off
```

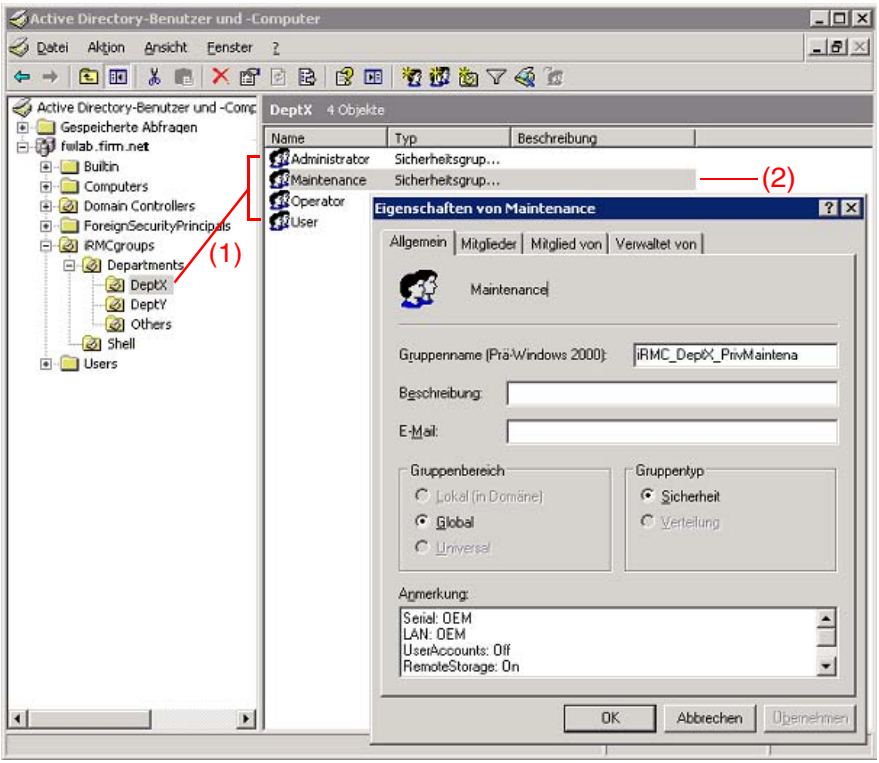


Bild 18: Eigenschaften-Dialogbox der Sicherheitsgruppe Maintenance

4.4.2.3 Einstellungen für die bevorzugte Shell

Im LDAP Server können Sie neben den Benutzerberechtigungen auch die bevorzugte Shell eines Benutzers festlegen. Anders als die Vergabe der Berechtigungen ist die Festlegung der bevorzugten Shell nur benutzerspezifisch, aber nicht abteilungsabhängig.

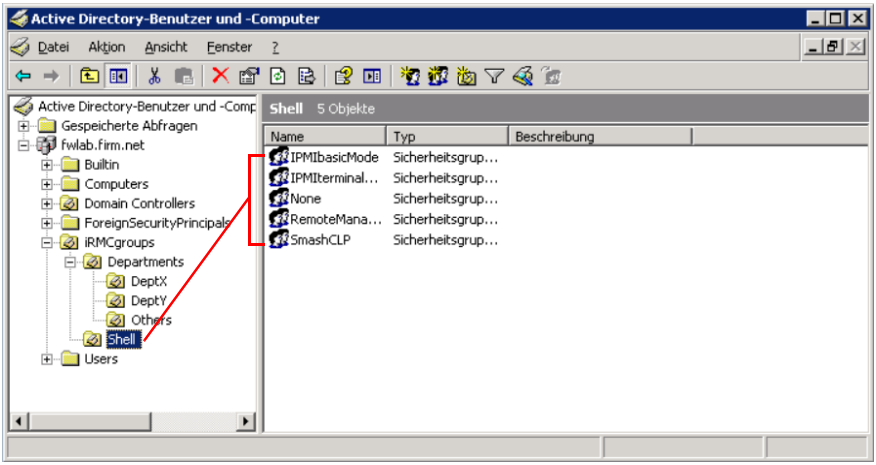


Bild 19: Bevorzugte Benutzershell festlegen

Folgende Gruppen stehen zur Auswahl:

– *IPMIbasicMode*

– *IPMIterminalMode*

– *None*

– *RemoteManager* (siehe Seite 307).

– *SmaschCLP* (siehe Seite 327).

Ein Benutzer sollte nur einer einzigen Shell-Gruppe angehören. Gehört ein Benutzer zu mehreren Shell-Gruppen, so wird er automatisch der Gruppe mit der höchsten Priorität unter diesen Gruppen zugeordnet. Die Prioritätenreihenfolge ist dabei durch die obige Liste vorgegeben (mit abnehmender Priorität von oben nach unten).

Ein Benutzer, der keiner Shell-Gruppe angehört, wird standardmäßig der Gruppe *Remote Manager* zugeordnet.

4.4.3 Struktur „iRMCgroups“ im LDAP Directory Service generieren

Damit Sie die globale iRMC-Benutzerverwaltung über einen Directory Service abwickeln können, müssen Sie die Struktur (OU) *iRMCgroups* im Directory Service generieren.

Hierfür gehen Sie wie folgt vor:

1. LDIF (**L**ightweight **D**irectory **I**nterchange **F**ormat)-Datei erstellen, die die iRMC-spezifischen Strukturen für die Integration in den Directory Service enthält.
2. LDIF-Datei in den Directory Service importieren.

4.4.3.1 LDIF-Datei erstellen

Die LDIF-Datei (*.ldif*) erstellen Sie mithilfe des Tools iRMCldifCreate aus einer Konfigurationsdatei (*.txt*).

Das Tool iRMCldifCreate finden Sie im Firmware-Package auf der ServerStart Update DVD.

iRMCldifCreate erzeugt alle benötigten Unterbäume inklusive aller Gruppen, nicht jedoch die Beziehungen zwischen Benutzern und Gruppen.

Die Erstellung und Zuordnung von Benutzereinträgen zu Gruppen nehmen Sie über ein entsprechendes Tool des verwendeten Directory Service vor, nachdem Sie die OU *iRMCgroups* im Directory Service generiert und den LDAP-Zugriff des iRMC auf den Directory Service konfiguriert haben.

Im Einzelnen gehen Sie bei der Erstellung der LDIF-Datei wie folgt vor:

► Erstellen Sie die Konfigurationsdatei (*.txt*) als Eingabedatei für das Tool iRMCldifCreate. Diese Textdatei enthält die Strukturinformationen für die Struktur *iRMCgroups* in lesbarer Form.

Die Syntax der Konfigurationsdatei ist in der Beispiel-Konfigurationsdatei beschrieben, die zusammen mit dem Programm iRMCldifCreate ausgeliefert wird.

Auf Seite 77 finden Sie ein Beispiel für eine Konfigurationsdatei.

Beispiel: Konfigurationsdatei

Nachfolgend ist ein Beispiel für eine Konfigurationsdatei abgedruckt:

```
#-------------------------------------------------------
# Configuration file for tool iRMCldifCreate
#-------------------------------------------------------


# Comment lines start with '#'
# Blank lines are also considered as comment
# Keywords for section start are enlosed in []


[Version]
# Version of config file syntax
1.1


[DirectoryServiceType]
# Type of directory service which should be used for iRMC
# Valid types: "Active Directory" - "Novell" - "OpenLDAP"
Active Directory


[BaseDN]
# LDAP notation of root path to domain without hostname
# No blanks allowed
# --- !!! Needs to be changed !!! ---
Dc=myorganization,dc=mycompany


[Departments]
# any number of departments possible
# name length is limited to 32 characters
# Department "Others" is optional
Others
# --- !!! Should be changed !!! ---
DeptX
DeptY


[Privileges]
# Table
# The table starts with a header containing the department,
# the group name and the privilege names
# A character '|' in the header marks that the column name is
# defined in a previous line
# The table body is separated by a new section recognized by
# section name with minimum 3 dashes e.g. [-----]
# Blanks and tabs can be used to separate the entries
# Group names must differ in the first 8 characters
# A department name "@all" marks that this group should be
# created for all departments

                                                  UserAccounts
                                                  |    iRMCsettings
                                                  |    |    VideoRedirection
Department   Groupname       LAN        Serial    |    |    |    RemoteStorage
[-------------------------------------------------------------------------------]
@all         Administrator   OEM        OEM       On   On   On   On
@all         Maintenance     OEM        OEM       Off  On   On   Off
@all         Operator        Operator   Operator  Off  Off  On   Off
@all         User            User       User      Off  Off  Off  Off
# --- !!! Should be changed !!! ---
DeptX        UserKVM         User       User      Off  Off  On   Off
```

► Rufen Sie das Tool iRMCldifCreate in der Windows Eingabeaufforderung mit folgender Syntax auf:

```
iRMCldifCreate [-v] [-h] [-d <display_level>]
   [-c <cfg_file>] [-o <out_file>] [-l <log_file>]
```

-v Aktuelle Programmversion anzeigen.

-h Aktuelle Nutzung des Programms anzeigen.

-d <display_level>
Display Level; steuert den Umfang der Programmausgabe auf Text-Konsole und in Logging-Datei.
Folgende Display Level werden unterschieden:
0: Es werden nur Fehler und Status-Meldungen angezeigt.
1: Zusätzlich zu Level 0 werden OUs und Gruppennamen angezeigt.
2: Zusätzlich zu Level 1 werden Attributwerte angezeigt.
Default: 1

-c <cfg_file>
Name der Konfigurationsdatei.
Default: *iRMCldifConfig.txt*

-o <out_file>
Name der LDIF-Datei.
Default: *iRMCdirServiceInit.ldif*

-l <log_file> | none
Name der Logging-Datei von iRMCldifCreate.
none: Es wird keine Loggingdatei geschrieben.
Default: *iRMCldifCreateLog.txt*

Alternativ können Sie dasTool iRMCldifCreate auch aus dem Windows Explorer heraus per Doppelklick auf die Datei *iRMCldifCreate.exe* aufrufen. In diesem Fall werden die Default-Werte verwendet.

Beispiel

Der folgende Aufruf erzeugt aus der Konfigurationsdatei *config_ldif.txt* die LDIF-Datei *ctrl.ldif*:

```
iRMCldifCreate -c config_ldif.txt -o ctrl.ldif
```

4.4.3.2 LDIF-Datei in den Directory Service importieren

Für den Import einer LDIF-Datei stehen je nach verwendetem Directory Service unterschiedliche Tools zur Verfügung.

Empfehlenswerte Tools sind u.a.:

- **Active Directory:** LDAP Browser\Editor
  Näheres siehe „LDIF-Datei in Microsoft Active Directory importieren“ auf Seite 80.
- **eDirectory:** iManager - eDir Maintenance with ICE (Import Convert Export Wizard)
  Näheres siehe „LDIF-Datei in Novell eDirectory importieren“ auf Seite 114.
- **OpenLDAP:** ldapadd (Management Tools)
  Näheres siehe „LDIF-Datei in OpenLDAP importieren“ auf Seite 129.

4.4.4 iRMC-Benutzerverwaltung via Microsoft Active Directory

Dieser Abschnitt beschreibt, wie Sie die iRMC-Benutzerverwaltung in Microsoft Active Directory integrieren.

Voraussetzung:

LDIF-Datei ist erstellt (siehe Abschnitt „Struktur „iRMCgroups“ im LDAP Directory Service generieren“ auf Seite 76).

Zur Integration der iRMC-Benutzerverwaltung in Microsoft Active Directory führen Sie die folgenden Schritte durch:

1. LDIF-Datei in Active Directory importieren.
2. iRMC-Benutzer den iRMC-Benutzergruppen in Active Directory zuordnen.
3. LDAP/SSL-Zugriff des iRMC am Active Directory Server konfigurieren.

4.4.4.1 LDIF-Datei in Microsoft Active Directory importieren

Für den Import einer LDIF-Datei in Active Directory stehen u.a. folgenden Tools zur Verfügung:

– Kommandozeilen-Tool „ldifde“ von Microsoft
– Programm „LDAP Administrator“ (professionelles Tool, lizenzpflichtig) der Firma Softerra
– „LDAP browser\editor“ mit LDIF Import-Funktionalität (von Jarek Gawor)

Im Folgenden sind nur das Kommandozeilen-Tool „ldifde“ von Microsoft und der „Open LDAP browser\editor“ von Jarek Gawor beschrieben, da die Nutzung dieser Tools keine zusätzlichen Kosten verursacht.

Kommandozeilen-Tool ldifde von Microsoft

ldifde ist ein Microsoft-Tool, das in der Windows-Eingabeaufforderung aufgerufen wird und unter Windows Server 2003 und Windows XP Professional ablauffähig ist.

Die Syntax von ldifde lautet wie folgt:

```
ldifde [-i] [-f <Dateiname>] [-s <Servername>]
       [-c <Zeichenfolge1> <Zeichenfolge2>] [-v] [-j <Pfad>]
       [-t <Portnummer>] [-d <BasisDN>] [-r <LDAPFilter>]
       [-p <Bereich>] [-l <LDAPAttributliste>]
       [-o <LDAPAttributliste>] [-g] [-m] [-n] [-k]
       [-a <BenutzerDN> <Kennwort>]
       [-b <Benutzername> <Domäne> <Kennwort>] [-?]
```

Eine Beschreibung der Operanden finden Sie in der Microsoft Online Dokumentation.

Für den Update eines Benutzereintrags vom Remote Arbeitsplatz aus rufen Sie ldifde wie folgt auf:

```
ldifde -i -f <ldif filename> -s <servername>
       -b <username> <domain> <password>
       -j <directory for log file> -k
```

Beispiel

```
ldifde -i -f iRMCdirServiceInit.ldif
       -s domino.fwlab.firm.net
       -b Administrator fwlab.firm.net my_password
       -j . -k
```

LDAP Browser\Editor von Jarek Gawor

Den LDAP Browser\Editor von Jarek Gawor können Sie über eine grafische Oberfläche einfach bedienen.

Das Tool steht zum Download zur Verfügung unter:

http://www-unix.mcs.anl.gov/~gawor/ldap/

Zur **Installation des LDAP Browser\Editor** verfahren Sie wie folgt:

- Entpacken Sie das Zip-Archiv *Browser281.zip* in ein Installationsverzeichnis Ihrer Wahl.
- Setzen Sie die Umgebungsvariable *JAVA_HOME* auf das Installationsverzeichnis der JAVA-Laufzeitumgebung, z.B.:

  ```
  JAVA_HOME=C:\Programme\Jave\jdk1.5.0_06
  ```

Zum **Importieren der LDIF-Datei in Active Directory** verfahren Sie wie folgt:

- Öffnen Sie den Open LDAP Browser\Editor.

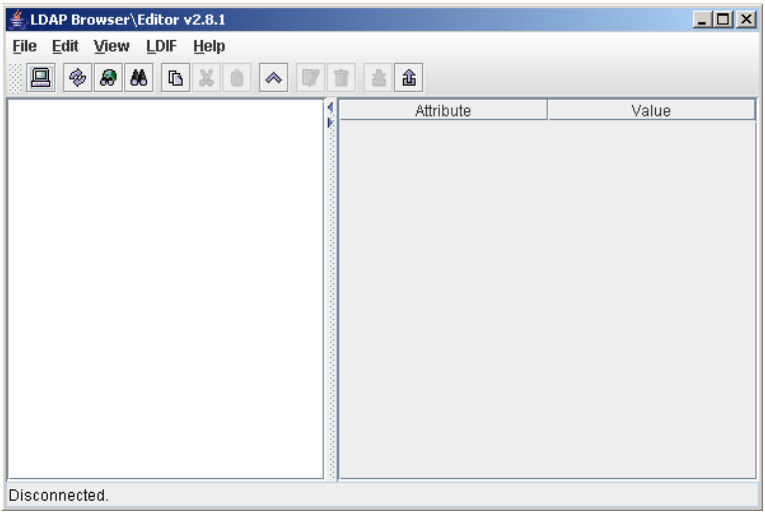


Bild 20: Open LDAP Browser\Editor

- Wählen Sie: *File - Connect - Session List - New*

  Die *Edit Session*-Dialogbox wird angezeigt (siehe Bild 21 auf Seite 83).

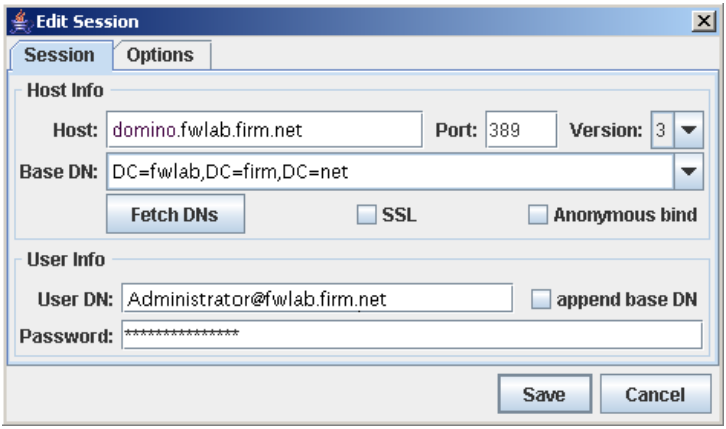


Bild 21: Open LDAP Browser\Editor - Edit Session

Host:
DNS Name oder IP-Adresse des Domain Controller

Port:
Portnummer 389 für Datenaustausch via LDAP

Version:
Versionsnummer (Wählen Sie 2 oder 3.)

Base DN:
Vollqualifizierter Domänenname, dargestellt als LDAP DN Name. Alternativ klicken Sie auf die Schaltfläche *Fetch DNs*.

Fetch DNs
Wenn Sie auf die Schaltfläche *Fetch DNs* klicken, wird eine Liste von DN Namen angezeigt, die u.a. auch den vollqualifizierten Domänennamen (dargestellt als LDAP DN Name) enthält.

User DN:
Login-Name des Benutzers, erweitert um „@“ und den vollen Pfadnamen der Domäne.

► Klicken Sie auf die Schaltfläche *Save*.

Der Open LDAP Browser/Editor zeigt das folgende Fenster an (siehe Bild 22 auf Seite 84):

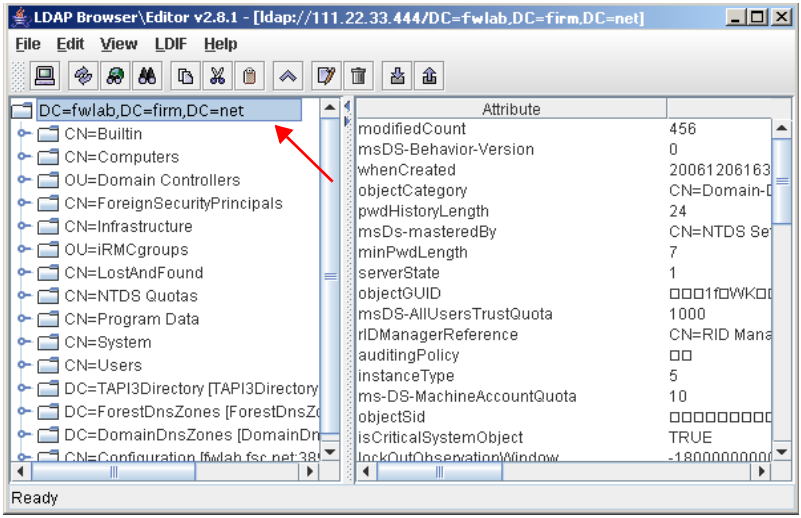


Bild 22: Top Level DN auswählen

► Markieren Sie den Top Level DN.

► Wählen Sie in der Menüleiste *LDIF - Import*.

Die Dialogbox *LDIF Import* wird angezeigt:

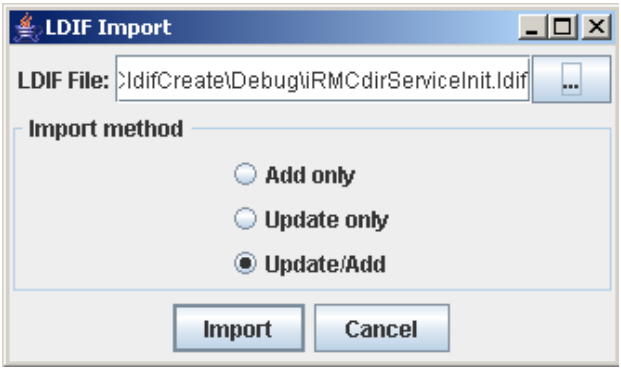


Bild 23: Import der LDIF-Datei starten

LDIF File:
LDIF-Datei, die zuvor mit dem Tool iRMCldifCreate erzeugt wurde.

Import method
Wählen Sie die *Update/Add*-Methode, um den *iRMCgroups*-Baum hinzuzufügen und/oder zu ändern.

► Klicken Sie auf die Schaltfläche *Import*, um den Import der LDIF-Datei in Active Directory zu starten.

4.4.4.2 LDAP/SSL-Zugriff des iRMC am Active Directory Server konfigurieren

Die iRMC-LDAP-Integration verwendet die auf dem OpenSSL Project basierende SSL Implementation von Eric Young. Einen Abdruck des SSL Copyrights finden Sie auf Seite 134.

Die Nutzung von LDAP via SSL durch den iRMC erfordert die Erstellung eines RSA-Zertifikats.

Die Konfiguration des LDAP-Zugriffs umfasst die folgenden Schritte:

1. Enterprise CA installieren.
2. RSA-Zertifikat für den Domain Controller erzeugen.
3. RSA-Zertifikat auf dem Server installieren.

Enterprise CA installieren

Eine CA ist eine „Zertifizierungsstelle für Zertifikate“. Eine Enterprise CA („Zertifizierungsstelle für Unternehmen“) können Sie wahlweise auf dem Domain Controller selbst oder auf einem anderen Server installieren.

Die Installation direkt auf dem Domain Controller ist einfacher, da im Vergleich zur Installation auf einem anderen Server einige Installationsschritte entfallen.

Im Folgenden ist beschrieben, wie Sie die Enterprise CA direkt auf einem vom Domain Controller verschiedenen Server installieren.

Die erfolgreiche Installation und Konfiguration einer Enterprise CA setzt eine Active Directory-Umgebung sowie die installierten IIS (**I**nternet **I**nformation **S**ervices) voraus.

Mit den folgenden Schritten installieren Sie eine Enterprise CA:

- Wählen Sie im Windows Startmenü:

  Start - Systemsteuerung - Software - Windows-Komponenten hinzufügen/entfernen

- Wählen Sie im Wizard für die Windows-Komponenten unter *Komponenten* den Punkt *Zertifikatsdienste*.
- Führen Sie einen Doppelklick auf *Zertifikatsdienste* aus und stellen Sie sicher, dass die Optionen *Webregistrierung für Zertifikatsdienste* und *Zertifizierungsstelle für Zertifikate* ausgewählt sind.
- Wählen Sie *Stammzertifizierungsstelle eines Unternehmens*.

- Aktivieren Sie die Option *Schlüsselpaar und Zertifizierungsstellenzertifikat mit diesen Einstellungen erstellen*.
- Wählen Sie *Microsoft Base DSS Cryptographic Provider*, um DSA-Zertifikate mit einer Schlüssellänge von 1024 Byte zu generieren.
- Exportieren Sie das öffentliche Zertifizierungsstellenzertifikat (CA Certificate).

  Im Einzelnen verfahren Sie hierfür wie folgt:

  - Starten Sie die Management-Konsole durch Eingabe von *mmc* in der Windows Eingabeaufforderung.
  - Fügen Sie das Snap-in für Zertifikate des lokalen Computers hinzu.
  - Navigieren Sie zu *Zertifikate (Lokaler Computer) - Vertrauenswürdige Stammzertifizierungsstellen - Zertifikate* und führen Sie einen Doppelklick aus.
  - Führen Sie einen Doppelklick auf das Zertifikat der neu erstellten Zertifizierungsstelle aus.
  - Klicken Sie im Zertifikatsfenster auf die Registerkarte *Details*.
  - Klicken Sie auf *In Datei kopieren*.
  - Wählen Sie einen Dateinamen für das Zertifizierungsstellenzertifikat und klicken Sie auf *Fertig stellen*.
- Laden Sie das öffentliche Zertifizierungsstellenzertifikat auf dem Domain Controller in das Zertifikatsverzeichnis *Vertrauenswürdige Stammzertifizierungsstellen*.

  Im Einzelnen verfahren Sie hierfür wie folgt:

  - Übertragen Sie die Datei des Zertifizierungsstellenzertifikats auf den Domain Controller.
  - Öffnen Sie im Windows Explorer das Zertifikat der neu erstellten Zertifizierungsstelle.
  - Klicken Sie auf *Zertifikat installieren*.
  - Klicken Sie unter *Alle Zertifikate in folgenden Speicher speichern* auf *Durchsuchen* und wählen Sie *Vertrauenswürdige Stammzertifizierungsstellen*.
  - Starten Sie die Management Konsole durch Eingabe von *mmc* in der Windows Eingabeaufforderung.

- ► Fügen Sie das Snap-in für Zertifikate des lokalen Computers hinzu.
- ► Fügen Sie das Snap-in für Zertifikate des aktuellen Benutzers hinzu.
- ► Kopieren Sie das Zertifizierungsstellenzertifikat (CA Certificate) aus dem Verzeichnis *Vertrauenswürdige Stammzertifizierungsstellen* des aktuellen Benutzers in das Verzeichnis *Vertrauenswürdige Stammzertifizierungsstellen* des lokalen Computers.

Domain Controller-Zertifikat erzeugen

Mit den folgenden Schritten erstellen Sie ein RSA-Zertifikat für den Domain Controller:

- ► Erstellen Sie eine Datei *request.inf* mit dem folgenden Inhalt:

```
[Version]
Signature="$Windows NT$"
[NewRequest]
Subject = "CN=<full path of domain controller host>"
KeySpec = 1
KeyLength = 1024
Exportable = TRUE
MachineKeySet = TRUE
SMIME = FALSE
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic
Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0

[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1
; this is for Server Authentication
```

- ► Passen Sie in der Datei *request.inf* die Angaben bei „Subject=“ an den Namen des verwendeten Domain Controllers an, z.B. `Subject = "CN=domino.fwlab.firm.net".`
- ► Geben Sie in der Windows Eingabeaufforderung folgendes Kommando ein: *certreq -new request.inf request.req*
- ► Geben Sie im Browser der Zertifizierungsstelle folgende URL ein: *http://localhost/certsrv*
- ► Klicken Sie auf *Ein Zertifikat anfordern.*

- Klicken Sie auf *erweiterte Zertifikatsanforderung.*
- Klicken Sie auf *Reichen Sie eine Zertifikatsanforderung ein.*
- Kopieren Sie den Inhalt der Datei *request.req* in das Fenster *Gespeicherte Anforderungen*.
- Wählen Sie die Zertifikatsvorlage *Webserver*.
- Laden Sie das Zertifikat herunter und speichern Sie es ab (z.B. in der Datei *request.cer*).
- Geben Sie in der Windows Eingabeaufforderung folgendes Kommando ein: *certreq -accept request.cer*
- Exportieren Sie das Zertifikat mit dem privaten Schlüssel.

  Im Einzelnen verfahren Sie hierfür wie folgt:

  - Starten Sie die Management Konsole durch Eingabe vom *mmc* in der Windows Eingabeaufforderung.
  - Fügen Sie das Snap-in für Zertifikate des lokalen Computers hinzu.
  - Navigieren Sie zu *Zertifikate (Lokaler Computer) - Eigene Zertifikate - Zertifikate*.
  - Führen Sie einen Doppelklick auf das neue Serverauthentifizierungs-Zertifikat aus.
  - Klicken Sie im Zertifikatsfenster auf die Registerkarte *Details*.
  - Klicken Sie auf *In Datei kopieren.*
  - Wählen Sie *Ja, privaten Schlüssel exportieren*.
  - Vergeben Sie ein Passwort.
  - Wählen Sie einen Dateinamen für das Zertifikat und klicken Sie auf *Fertig stellen*.

Domain Controller-Zertifikat auf dem Server installieren

Mit den folgenden Schritten installieren Sie das Domain Controller-Zertifikat auf dem Server:

- ► Kopieren Sie die soeben erstellte Datei für das Domain Controller-Zertifikat auf den Domain Controller.
- ► Führen Sie einen Doppelklick auf das Domain Controller-Zertifikat aus.
- ► Klicken Sie auf *Zertifikat installieren.*
- ► Verwenden Sie das Passwort, das Sie beim Export der Zertifikats vergeben haben.
- ► Klicken Sie unter *Alle Zertifikate in folgendem Speicher speichern* auf die Schaltfläche *Durchsuchen* und wählen Sie *Eigene Zertifikate*.
- ► Starten Sie die Management Konsole durch Eingabe von *mmc* in der Windows Eingabeaufforderung.
- ► Fügen Sie das Snap-in für Zertifikate des lokalen Computers hinzu.
- ► Fügen Sie das Snap-in für Zertifikate des aktuellen Benutzers hinzu.
- ► Kopieren Sie das Domain Controller-Zertifikat aus dem Verzeichnis *Eigene Zertifikate* des aktuellen Benutzers in das Verzeichnis *Eigene Zertifikate* des lokalen Computers.

4.4.4.3 iRMC-Benutzer der OU „iRMCgroups“ zuordnen

Die Zuordnung von iRMC-Benutzern zu iRMC-Gruppen in der OU *iRMCgroups* können Sie wahlweise vornehmen

– ausgehend vom Benutzereintrag oder
– ausgehend vom Gruppeneintrag.

Nachfolgend ist die Zuordnung ausgehend vom der Gruppeneintrag beschrieben. Die Zuordnung ausgehend vom Benutzereintrag verläuft weitgehend analog.

In Active Directory müssen die Benutzer „von Hand“ in die Gruppen eingetragen werden.

Gehen Sie wie folgt vor:

► Öffnen Sie das Snap-in *Active Directory-Benutzer und -Computer.*

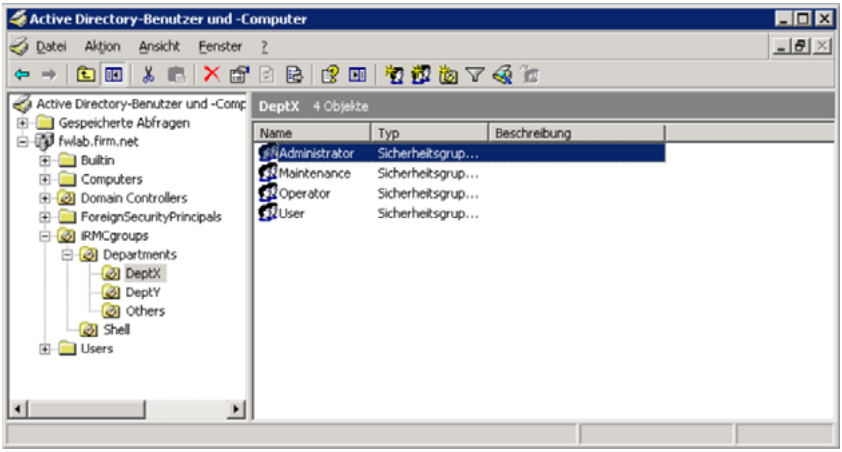


Bild 24: Snap-in Active Directory-Benutzer und -Computer

► Führen Sie einen Doppelklick auf die Gruppe (hier: Administrator) aus.

Die Dialogbox *Eigenschaften von Administrator* wird geöffnet (siehe Bild 25 auf Seite 92).

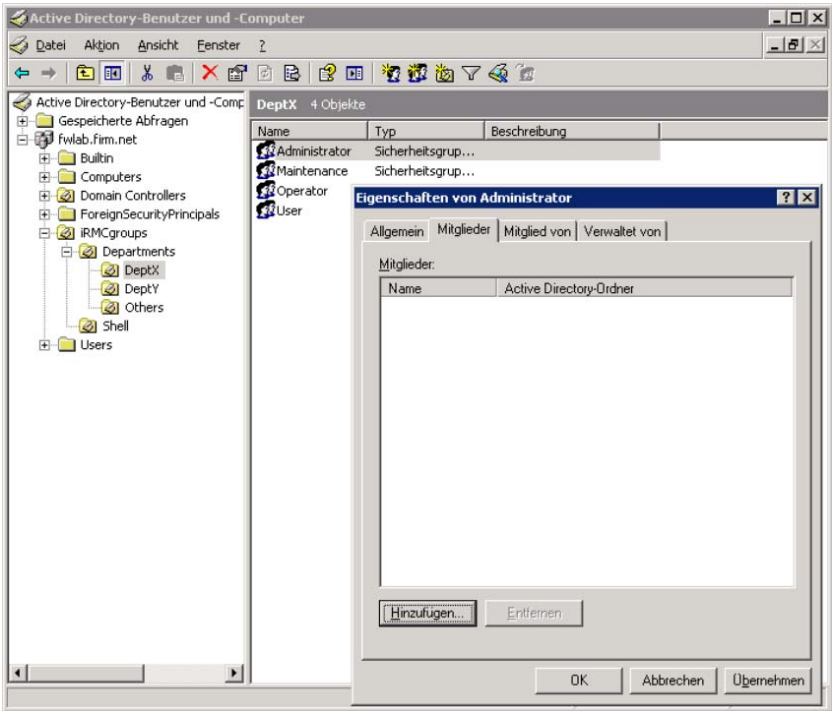


Bild 25: Dialogbox Eigenschaften von Administrator

- Wählen Sie die Registerkarte *Mitglieder*.
- Klicken Sie auf die Schaltfläche *Hinzufügen...* .

  Die Dialogbox *Benutzer, Kontakte oder Computer wählen* wird geöffnet (siehe Bild 26 auf Seite 93).

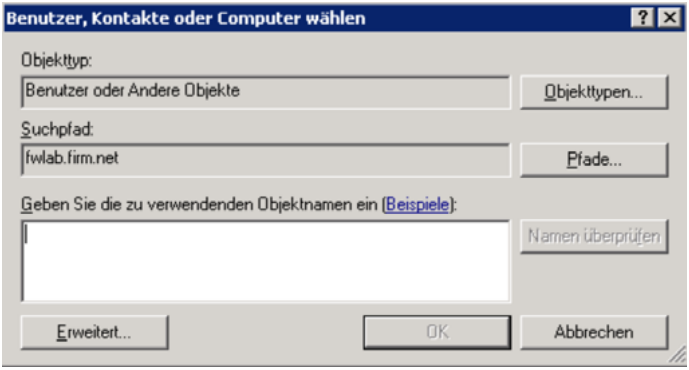


Bild 26: Dialogbox Benutzer, Kontakte oder Computer wählen

► Klicken Sie auf die Schaltfläche *Pfade...* .

Die Dialogbox *Pfad* wird geöffnet.

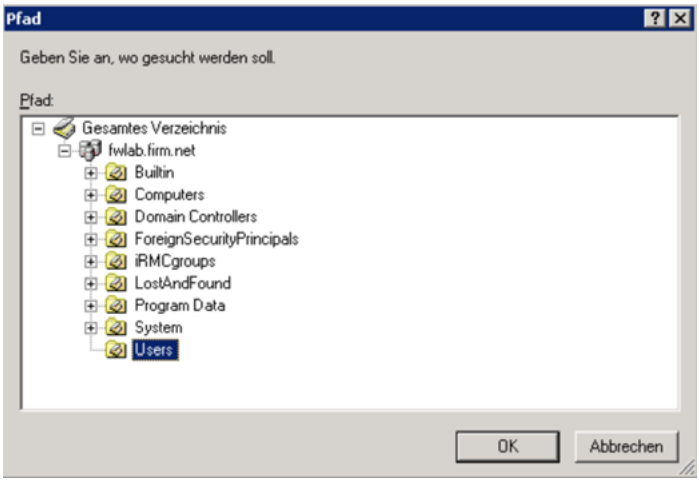


Bild 27: Dialogbox Pfad

► Selektieren Sie den Container (OU), in dem sich Ihre Benutzer befinden. (Im Standardfall ist dies die OU *Users*.) Bestätigen Sie mit *OK*.

Die Dialogbox *Benutzer, Kontakte und Computer wählen* wird geöffnet (siehe Bild 28 auf Seite 94).

Benutzer können auch an anderer Stelle im Directory eingetragen sein.

Bild 28: Dialogbox Benutzer, Kontakte oder Computer wählen

► Klicken Sie auf die Schaltfläche *Erweitert...* .

Eine erweiterte Dialogbox Benutzer, Kontakte und Computer wählen wird geöffnet (siehe Bild 29 auf Seite 95).

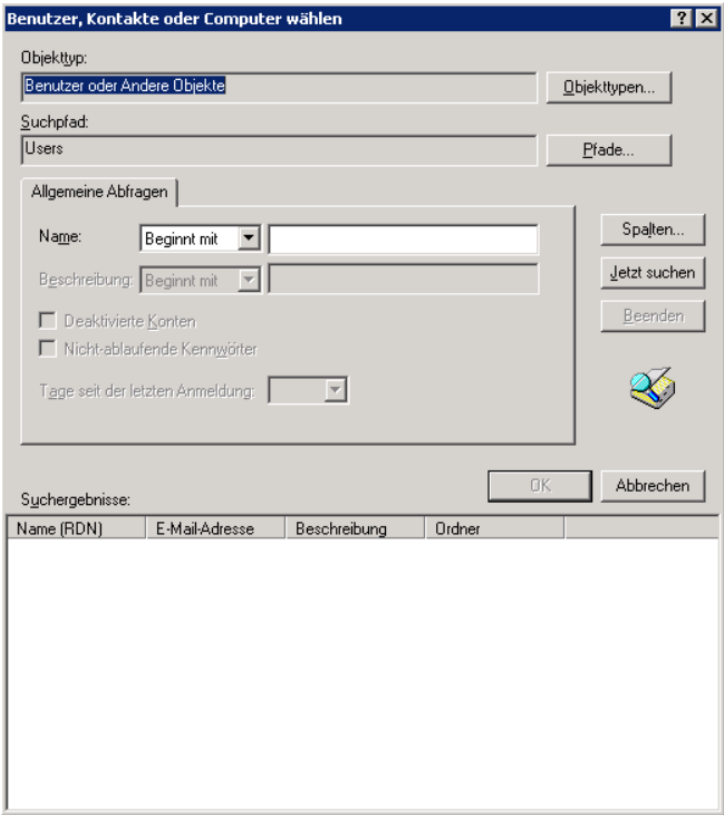


Bild 29: Dialogbox Benutzer, Kontakte oder Computer wählen - Suchen

► Klicken Sie auf die Schaltfläche *Jetzt suchen*, um sich alle Benutzer Ihrer Domäne anzeigen zu lassen.

Im Anzeigebereich unter *Suchergebnisse:* wird das Suchergebnis angezeigt (siehe Bild 30 auf Seite 96).

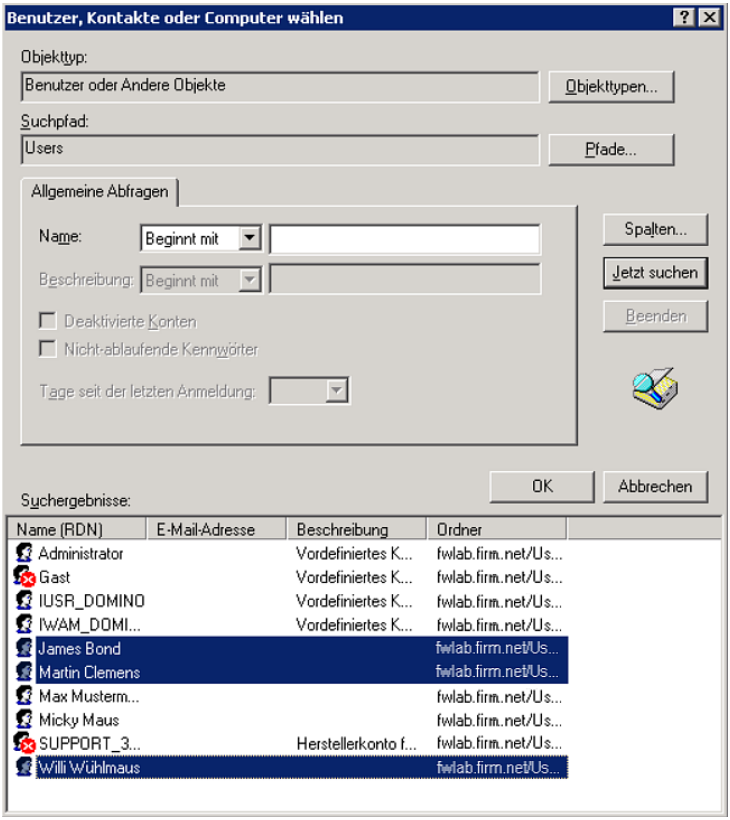


Bild 30: Dialogbox Benutzer, Kontakte oder Computer wählen - Suchergebnisse anzeigen

► Selektieren Sie die Benutzer, die zur Gruppe hinzugefügt werden sollen, und bestätigen Sie mit *OK*.

Es werden nun die ausgewählten Benutzer angezeigt (siehe Bild 31 auf Seite 97).

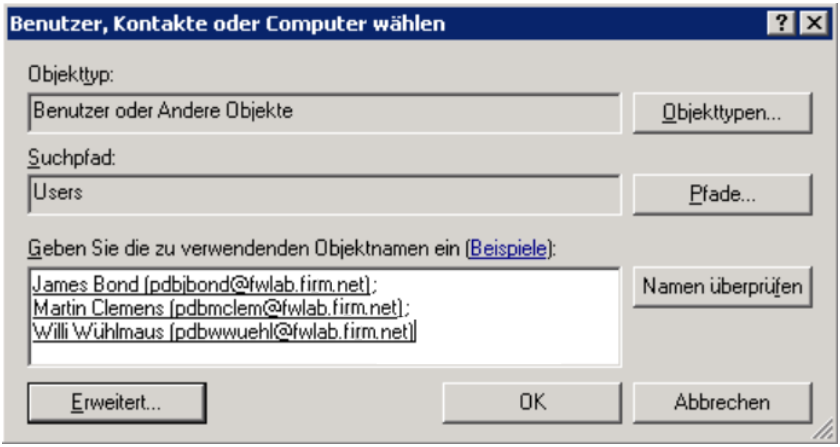


Bild 31: Dialogbox Benutzer, Kontakte oder Computer wählen - Suchergebnisse bestätigren

► Bestätigen Sie mit *OK*.

4.4.5 iRMC-Benutzerverwaltung via Novell eDirectory

Dieser Abschnitt informiert über die folgenden Themen:

– Software-Komponenten und Systemanforderungen von Novell eDirectory

– Novell eDirectory installieren.

– Novell eDirectory konfigurieren.

– iRMC-Benutzerverwaltung in Novell eDirectory integrieren.

– Tipps zur Administration von Novell eDirectory.

Installation und Konfiguration von Novell eDirectory werden im Folgenden ausführlich beschrieben. Tiefere eDirectory-Kenntnisse werden nicht vorausgesetzt. Sofern Sie bereits mit Novell eDirectory vertraut sind, können Sie die folgenden drei Abschnitte überspringen und fortfahren mit Abschnitt „iRMC-Benutzerverwaltung in Novell eDirectory integrieren“ auf Seite 112.

4.4.5.1 Software-Komponenten und Systemanforderungen

Verwenden Sie jeweils die angegebene oder eine aktuellere Version der nachfolgend aufgelisteten Komponenten.

Novell eDirectory (ehemals NDS) besteht aus folgenden Software-Komponenten:

– eDirectory 8.8: *20060526_0800_Linux_88-SP1_FINAL.tar.gz*

– eDirectory 8.8: *eDir_88_iMan26_Plugins.npm*

– iManager: *iMan_26_linux_64.tgz* für SuSE, *iMan_26_linux_32.tgz* sonst

– ConsoleOne: *c1_136f-linux.tar.gz*

Für Installation und Betrieb von Novell eDirectory gelten die folgenden Systemanforderungen:

– OpenSSL muss installiert sein.

  Falls OpenSSL nicht bereits installiert ist:

  ► Installieren Sie OpenSSL, **bevor** Sie mit der Installation von Novell eDirectory beginnen.

– 512 MB freier Hauptspeicher

4.4.5.2 Novell eDirectory installieren

Die Installation von Novell eDirectory umfasst die Installation der folgenden Komponenten:

– eDirectory Server und Administrations-Utilities

– iManager (Administrations-Utility)

– ConsoleOne (Administrations-Utility)

Voraussetzung für die Installation von Novell eDirectory:

– Ein Linux Server-Betriebssystem muss komplett installiert sein und laufen.

– Die Firewall muss für Verbindungen zu folgenden Ports konfiguriert sein: 8080, 8443, 9009, 81, 389, 636.

  Für OpenSuSE konfigurieren Sie dies mithilfe der Datei */etc/sysconfig/SuSEfirewall2*:

  ► Erweitern Sie in der Datei */etc/sysconfig/SuSEfirewall2* den Eintrag *FW_SERVICES_EXT_TCP* wie folgt:

  ```
  FW_SERVICES_EXT_TCP="8080 8443 9009 81 389 636"
  ```

– Gemäß dem eDirectory Installation Guide muss das System für Multicast Routing eingerichtet sein.

  Für SuSE Linux gehen Sie hierfür wie folgt vor:

  ► Erzeugen oder (sofern bereits vorhanden) öffnen Sie die Datei */etc/sysconfig/network/ifroute-eth0*.

  ► Erweitern Sie */etc/sysconfig/network/ifroute-eth0* um die folgende Zeile:

  ```
  224.0.0.0  0.0.0.0  240.0.0.0  eth0
  ```

  Dadurch passen Sie *eth0* der Systemkonfiguration an.

Voraussetzungen für die Installation des eDirectory Servers, der eDirectory Utilities, des iManager und von ConsoleOne:

- Für die Installation ist Root-Berechtigung erforderlich.
- Die im Folgenden beschriebene Vorgehensweise bei der Installation setzt voraus, dass alle für die Installation benötigten Dateien bereits in ein Verzeichnis (z.B. */home/eDirectory*) kopiert wurden. Es handelt sich dabei um folgende Dateien:

  20060526_0800_Linux_88-SP1_FINAL.tar.gz
  iMan_26_linux_64.tgz
  c1_136f-linux.tar.gz

eDirectory Server und Administrations-Utilities installieren

Gehen Sie wie folgt vor:

- Melden Sie sich mit Root-Berechtigung (Super User) an.
- Wechseln Sie in das Verzeichnis, das die für die Installation benötigten Dateien enthält (im Beispiel: */home/eDirectory*):

  ```
  cd /home/eDirectory
  ```

- Extrahieren Sie das Archiv *20060526_0800_Linux_88-SP1_FINAL.tar.gz*:

  ```
  tar -xzvf 20060526_0800_Linux_88-SP1_FINAL.tar.gz
  ```

  Nach der Extraktion enthält */home/eDirectory* ein neues Unterverzeichnis *eDirectory*.

eDirectory Server installieren

- Wechseln Sie in das Unterverzeichnis *setup* dieses *eDirectory*-Verzeichnisses:

  ```
  cd eDirectory/setup
  ```

- Rufen Sie das Installationsskript *./nds-install* auf:

  ```
  ./nds-install
  ```

- Akzeptieren Sie die EULA mit „y“ und bestätigen Sie mit der Enter-Taste.
- Wenn Sie nach dem zu installierenden Programm gefragt werden:

  Geben Sie „1“ ein für die **Installation des Novell eDirectory Servers** und bestätigen Sie der Enter-Taste.

  Daraufhin werden die eDirectory-Packages installiert.

Nach der Installation des Novell eDirectory Servers müssen Sie in einigen Umgebungsvariablen die Namen für die Pfade auf das eDirectory aktualisieren und die Variablen exportieren.

- Öffnen Sie hierfür Ihre Konfigurationsdatei (im Beispiel: */etc/bash.bashrc*) und fügen Sie die dort vor „# End of ..." die folgenden Zeilen in der angegebenen Reihenfolge ein:

```
export PATH/opt/novell/eDirectory/bin:/opt/novell/eDirectory/
       sbin:$PATH

export LD_LIBRARY_PATH=/opt/novell/eDirectory/lib:/
       opt/novell/eDirectory/lib/nds-modules:/opt/novell/
       lib:$LD_LIBRARY_PATH

export MANPATH=/opt/novell/man:/opt/novell/eDirectory/
       man:$MANPATH

export TEXTDOMAINDIR=/opt/novell/eDirectory/share/
       locale:$TEXTDOMAINDIR
```

- Schließen Sie das Terminal und öffnen Sie ein neues Terminal, um die Umgebungsvariablen zu exportieren.

eDirectory Administrations-Utilities installieren

- Wechseln Sie in das Unterverzeichnis *setup* des *eDirectory*-Verzeichnisses:

```
cd eDirectory/setup
```

- Rufen Sie das Installationsskript auf:

```
./nds-install
```

- Akzeptieren Sie die EULA mit „y" und bestätigen Sie mit der Enter-Taste.
- Wenn Sie nach dem zu installierenden Programm gefragt werden:

  Geben Sie „2" ein für die **Installation der Novell eDirectory Administrations-Utilities** und bestätigen Sie der Enter-Taste.

  Daraufhin werden die eDirectory Administrations-Utilities installiert.

iManager installieren und aufrufen

Der iManager ist das für die Administration von Novell eDirectory empfohlene Tool. Für die Installation sowohl in SLES10 als auch in OpenSuSE verwenden Sie das Archiv **_64.tgz*.

Gehen Sie wie folgt vor:

- Melden Sie sich mit Root-Berechtigung (Super User) an.
- Wechseln Sie in das Verzeichnis */home/eDirectory*:

  ```
  cd /home/eDirectory
  ```

- Extrahieren Sie das Archiv *iMan_26_linux_64.tgz*:

  ```
  tar -xzvf iMan_26_linux_64.tgz
  ```

  Nach der Extraktion enthält */home/eDirectory* ein neues Unterverzeichnis *iManager*.

- Wechseln Sie in das Unterverzeichnis *installs* von *iManager*:

  ```
  cd iManager/installs/linux
  ```

- Rufen Sie das Installationsskript auf:

  ```
  ./iManagerInstallLinux.bin
  ```

- Wählen Sie die Sprache, in der die Installationsmeldungen ausgegeben werden sollen.
- Klicken Sie durch die EULA und akzeptieren Sie die EULA.
- Wählen Sie *1- Novell iManager 2.6, Tomcat, JVM* zur iManager-Installation.
- Wählen Sie *1- Yes* für Plugin-Download.
- Drücken Sie auf Enter, um den Default-Pfad für den Download zu verwenden.

  Das Installationsprogramm sucht via Internet nach Downloads. Dies kann einige Minuten dauern. Danach werden Sie aufgefordert, die zu installierenden Plugins auszuwählen.

  - Wählen Sie *All* für den Download aller Plugins.
  - Wählen Sie *1- Yes* für die Installation der lokal verfügbaren Plugins.

- Drücken Sie auf Enter, um den Default-Pfad für die Installation zu verwenden.
- Wählen Sie *2- No* für die automatische Konfiguration von Apache (optional).

- Akzeptieren Sie den Default Port (8080) für Tomcat.
- Akzeptieren Sie den Default SSL-Port (8443) für Tomcat.
- Akzeptieren Sie den Default JK Connector-Port (9009) für Tomcat.
- Geben Sie die administrationsberechtigte Benutzerkennung (z.B. „root.firm“) für den administrationsberechtigten Benutzer ein.
- Geben Sie den Baumnamen (z.B. „fwlab“) für den administrationsberechtigten Benutzer ein.
- Akzeptieren die aufgelistete Zusammenfassung Ihrer Eingaben mit *1-OK...*, um die Installation abzuschließen.

Beim Novell iManager einloggen

Nach der Installation können Sie sich via Web-Browser mithilfe der folgenden URL am iManager einloggen:

https://<IP-Adresse des eDirectory-Servers>:8443/nps

Novell empfiehlt die Verwendung der Web-Browser Microsoft Internet Explorer oder Mozilla Firefox. In Mozilla Firefox werden möglicherweise nicht alle Popup-Fenster des Kontext-Menüs angezeigt.

ConsoleOne installieren und starten

Mit ConsoleOne steht Ihnen ein weiteres Administrationstool von Novell eDirectory zur Verfügung.

Zur Installation von ConsoleOne gehen Sie wie folgt vor:

- Melden Sie sich mit Root-Berechtigung (Super User) am eDirectory Server an.
- Wechseln Sie in das Verzeichnis */home/eDirectory*:

  ```
  cd /home/eDirectory
  ```

- Extrahieren Sie das ConsoleOne-Archiv *c1_136f-linux.tar.gz*:

  ```
  tar -xzvf c1_136f-linux.tar.gz
  ```

  Nach der Extraktion enthält */home/eDirectory* ein neues Verzeichnis *Linux*.

- Wechseln Sie in das Verzeichnis *Linux*:

  ```
  cd Linux
  ```

- Rufen Sie das Installationsskript *c1-install* auf:

  ```
  ./c1-install
  ```

- Wählen Sie die Sprache, in der die Installationsmeldungen ausgegeben werden sollen.
- Geben Sie „8“ für die Installation aller Snap-Ins ein.

ConsoleOne benötigt den Pfad zu einer installierten Java-Laufzeitumgebung. Den entsprechenden Pfadnamen können Sie in die Umgebungsvariable *C1_JRE_HOME* exportieren. Demgegenüber erfordert der systemweite Export des Pfadnamens Änderungen in der *bash*-Profile.

Da Root-Berechtigung für das Arbeiten mit ConsoleOne erforderlich ist, genügt es im Prinzip, den Pfadnamen nur für die Kennung *superuser Root* zu exportieren. Im Folgenden ist jedoch der systemweite Export des Pfadnamens dargestellt. Damit können auch normale Benutzer mit ConsoleOne arbeiten, sofern sie Root-Berechtigung besitzen.

Gehen Sie wie folgt vor:

- Öffnen Sie die Ihre Konfigurationsdatei zur Bearbeitung (im Beispiel: */etc/bash.bashrc*)
- Fügen Sie in der Konfigurationsdatei vor „# End of ...“ die folgende Zeile ein:

```
export C1_JRE_HOME=/opt/novell/j2sdk1.4.2_05/jre
```

> **i** Hier wird die zusammen mit eDirectory installierte Java-Laufzeitumgebung verwendet. Sie können aber auch den Pfadnamen einer beliebigen anderen auf dem eDirectory Server installierten Java-Laufzeitumgebung angeben.

ConsoleOne erhält die verfügbaren Baumstrukturen entweder über die lokale Konfigurationsdatei *hosts.nds* oder über den SLP-Service und Multicast.

Zum Einfügen Ihrer Baumstruktur in die Konfigurationsdatei gehen Sie verfahren Sie wie folgt:

- Wechseln Sie in Ihr Konfigurationsverzeichnis:

```
cd /etc
```

- Erzeugen Sie die Datei *hosts.nds*, falls Sie noch nicht existiert.
- Öffnen Sie die Datei *hosts.nds* und fügen Sie die folgenden Zeilen ein:

```
#Syntax: TREENAME.FQDN:PORT
MY_Tree.mycomputer.mydomain:81
```

ConsoleOne starten

ConsoleOne starten Sie in der System-Eingabeaufforderung mit folgendem Kommando:

```
/usr/ConsoleOne/bin/ConsoleOne
```

4.4.5.3 Novell eDirectory konfigurieren

Zur Konfiguration von Novell eDirectory führen Sie die folgenden Schritte durch:

1. NDS-Baum erzeugen.
2. eDirectory für LDAP konfigurieren.
3. Zugang zu eDirectory via LDAP-Browser testen.

NDS-Baum erzeugen

Einen NDS (**N**etwork **D**irectory **S**ervice)-Baum erzeugen Sie mit dem Utility ndsmanage. ndsmanage benötigt hierfür die folgenden Informationen:

TREE NAME
: Netzweit eindeutiger Name für den neuen NDS-Baum, z.B. *MY_TREE*.

Server Name
: Name einer Instanz der Klasse *server* in eDirectory. Für *Server Name* spezifizieren Sie den Namen des PRIMERGY Servers, auf dem der LDAP-Server läuft, z.B. *lin36-root-0*.

Server Context
: Fully Distinguished Name des Containers, in dem das *Server* Objekt enthalten ist, z.B. *dc=organization.dc=mycompany*.

Admin User
: Fully Distinguished Name des administrationsberechtigten Benutzers, z.B. *cn=admin.dc=organization.dc=mycompany*

NCP Port
: Spezifizieren den Port 81.

Instance Location
: Spezifizieren Sie als Pfad: */home/root/instance0*

Configuration File
: Spezifizieren Sie folgende Datei: */home/root /instance0/ndsconf*

Password for admin user
: Geben Sie hier das Administratorpasswort an.

Zur Konfigurierung des NDS-Baums gehen Sie wie folgt vor:

- ► Öffnen Sie eine Command Box.
- ► Wechseln Sie in das Verzeichnis */home/eDirectory*.
- ► Starten Sie das Utility ndsmanage durch Eingabe des Kommandos *ndsmanage*:

  ```
  ndsmanage
  ```

- ► Geben Sie „c“ ein für die Erzeugung einer neuen Instanz der Klasse *server*.
- ► Geben Sie „y“ ein , um die Konfiguration fortzusetzen.
- ► Geben Sie „y“ ein, um einen neuen Baum zu erzeugen.

  Anschließend erfragt ndsmanage nacheinander die Werte für *TREE NAME*, *Server Name*, *Server Context* etc. (siehe Seite 106).

  Sobald die Eingabe abgeschlossen ist, konfiguriert ndsmanage den NDS-Baum.

- ► Führen Sie nach Abschluss der Konfiguration des NDS-Baums einen Neustart des PRIMERGY Servers durch, um die Konfiguration zu aktivieren, d.h. den NDS-Baum zu erzeugen.

eDirectory für LDAP konfigurieren

Die Konfiguration von eDirectory für LDAP umfasst die folgenden Schritte:

- – Role Based Services (RBS) installieren.
- – Plugin-Module installieren.
- – Role Based Services (RBS) konfigurieren.
- – eDirectory mit/ohne SSL/TLS-Unterstützung konfigurieren.

Im Einzelnen gehen Sie wie folgt vor:

- ► Loggen Sie sich beim iManager via Web-Browser unter der Administratorkennung (*Admin*) ein.

Role Based Services (RBS) installieren

RBS installieren Sie mithilfe des iManager Configuration Wizard.

Gehen Sie wie folgt vor:

- ► Wählen Sie im iManager die Registerkarte *Configure* (durch Klicken auf das Desk-Symbol).

- ► Wählen Sie in der Registerkarte *Configure*:
  Role Based Services - *RBS Configuration*
- ► Starten Sie den RBS Configuration Wizard.
- ► Weisen *RBS2* dem zu verwaltenden Container zu. (Im obigen Beispiel ist dies „mycompany“.)

Plugin-Module installieren

Gehen Sie wie folgt vor:

- ► Wählen Sie im iManager die Registerkarte *Configure* (durch Klicken auf das Desk-Symbol).
- ► Wählen Sie in der Registerkarte *Configure*:
  Plug-in installation - *Available Novell Plug-in Modules*
- ► Wählen Sie in der Seite *Available Novell Plug-in Modules* unter den aufgelisteten Modulen das eDirectory-spezifische Package *eDir_88_iMan26_Plugins.npm*.
- ► Klicken Sie auf *Install*.

Role Based Services (RBS) konfigurieren

- ► Wählen Sie in der Seite *Available Novell Plug-in Modules* alle für die LDAP-Integration benötigten Module. Falls Sie sich nicht sicher sind, wählen Sie alle Module.
- ► Klicken Sie auf *Install*.

eDirectory für SSL/TLS gesicherten Zugriff konfigurieren

Während der eDirectory-Installation wird ein temporäres Zertifikat erzeugt, sodass der Zugriff auf eDirectory standardmäßig durch SSL/TLS abgesichert ist. Da jedoch die Firmware des iRMC für die Verwendung von RSA/MD5-Zertifikaten konfiguriert ist, benötigt die SSL/TLS gesicherte globale iRMC-Benutzerverwaltung via eDirectory ein RSA/MD5 Zertifikat der Länge 1024 byte.

Ein RSA/MD5-Zertifikat der Länge 1024 byte erstellen Sie wie folgt mithilfe von ConsoleOne:

- Loggen Sie sich am LDAP-Server unter Ihrer Administratorkennung (*Admin*) ein und starten Sie ConsoleOne.
- Navigieren Sie zum Root-Verzeichnis Ihrer Unternehmensstruktur (z.B. *baumname/mycompany/myorganisation*).
- Wählen Sie *New Object - NDSPKI key material - custom*, um ein neues Objekt der Klasse *NDSPKI:Key Material* zu erstellen.
- Spezifizieren Sie im nachfolgenden Dialog die folgenden Werte:

  1. 1024 bits
  2. SSL or TLS
  3. signature RSA/MD5

  Ein neues Zertifikat des gewünschten Typs wird erstellt.

Um das neu erstellte Zertifikat für die SSL-gesicherte LDAP-Verbindung zu aktivieren führen Sie im iManager die folgenden Schritte durch:

- Starten Sie den iManager via Web-Browser.
- Loggen Sie sich beim iManager mit gültigen Authentisierungsdaten ein.
- Wählen Sie *LDAP - LDAP Options - LDAP Server - Connection*.

  Die Registerkarte *Connection* enthält eine Drop down-Liste, die alle auf dem System installierten Zertifikate anzeigt.
- Selektieren Sie in der Drop down-Liste das gewünschte Zertifikat.

eDirectory für den nicht-SSL-gesicherten Zugriff konfigurieren

Anonymes Login sowie die Übertragung von Klartext-Passwörtern über ungesicherte Kanäle sind in eDirectory standardmäßig deaktiviert. Demzufolge ist das Einloggen via Web-Browser am eDirectory-Server nur über eine SSL-Verbindung möglich.

Für die Nutzung von LDAP ohne SSL müssen Sie die folgenden Schritte durchführen:

1. Nicht-SSL-gesicherte LDAP-Verbindung ermöglichen.
2. Bind-Restriktionen lockern.
3. LDAP-Konfiguration neu laden.

Gehen Sie wie folgt vor:

1. Nicht-SSL-gesicherte LDAP-Verbindung ermöglichen.
   - ► Starten Sie den iManager via Web-Browser.
   - ► Loggen Sie sich beim iManager mit gültigen Authentisierungsdaten ein.
   - ► Wählen Sie den *Roles and Tasks*-View.
   - ► Wählen Sie *LDAP - LDAP Options - LDAP Server - Connection*.
   - ► Deaktivieren in der Registerkarte *Connection* die Option *Require TLS for all Operations.*
   - ► Wählen Sie *LDAP - LDAP Options - LDAP Group - General*.
   - ► Deaktivieren die in der Registerkarte *General* die Option *Require TLS for Simple Binds with password.*
2. Bind-Restriktionen lockern.
   - ► Loggen Sie sich beim iManager mit gültigen Authentisierungsdaten ein.
   - ► Navigieren Sie im Objekt-Baum zum *LDAP Server*-Objekt.
   - ► Markieren Sie das *LDAP Server*-Objekt per Maus-Klick und wählen Sie *Modify Object* im zughörigen Kontext-Menü.
   - ► Öffnen Sie im rechten Content-Frame das *Other*-Sheet.
   - ► Wählen Sie unter *Valued Attributes*: *ldapBindRestrictions*
   - ► Klicken Sie auf die Schaltfläche *Edit*.
   - ► Setzen Sie den Wertauf „0“.
   - ► Klicken Sie auf die Schaltfläche *OK*.
   - ► Klicken Sie im *Other*-Sheet auf die Schaltfläche *Apply*.
3. LDAP-Konfiguration neu laden.
   - ► Starten Sie ConsoleOne und loggen Sie sich in eDirectory ein.
   - ► Klicken Sie auf der links im Fenster auf das *Base DN*-Objekt (z.B. *Mycompany*). Auf der rechten Fensterseite wird daraufhin das *LDAP Server*-Objekt angezeigt.
   - ► Markieren Sie das *LDAP Server*-Objekt per Klick mit der rechten Maustaste und selektieren Sie *Properties...* im zughörigen Kontext-Menü.
   - ► Klicken Sie in der Registerkarte *General* auf *Refresh NLDAP Server Now*.

Zugriff auf eDirectory via LDAP Browser testen

Nach erfolgreicher Durchführung der oben beschriebenen Schritte 1 - 3 sollten Sie via LDAP Browser-Utility eine Verbindung zu eDirectory herstellen können. Mit dem LDAP-Browser von Jarek Gavor können Sie dies wie folgt testen:

- Versuchen Sie, sich unter der Administratorkennung (im Beispiel: *admin*) über eine SSL-Verbindung in eDirectory einzuloggen.

Falls der Versuch fehlschlägt, verfahren Sie wie folgt:

- Prüfen Sie, ob SSL aktiviert ist (vergleiche Seite 109).

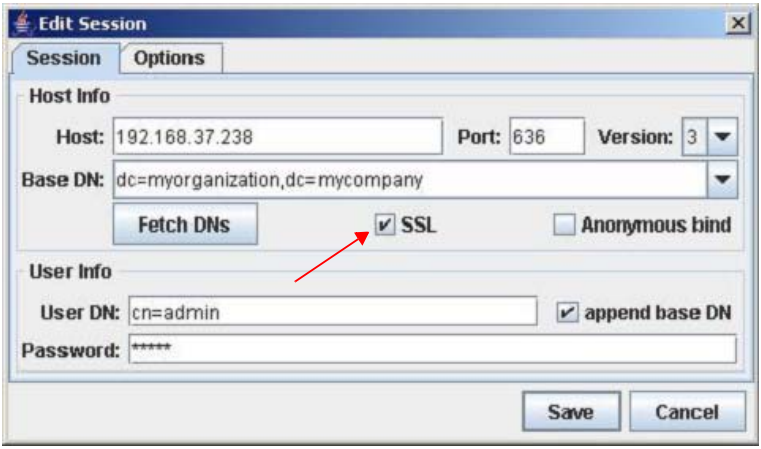


Bild 32: LDAP-Zugriff auf eDirectory testen: SSL aktiviert

- Versuchen Sie, sich unter der Administratorkennung (im Beispiel: *admin*) über eine nicht SSL-gesicherte Verbindung in eDirectory einzuloggen.

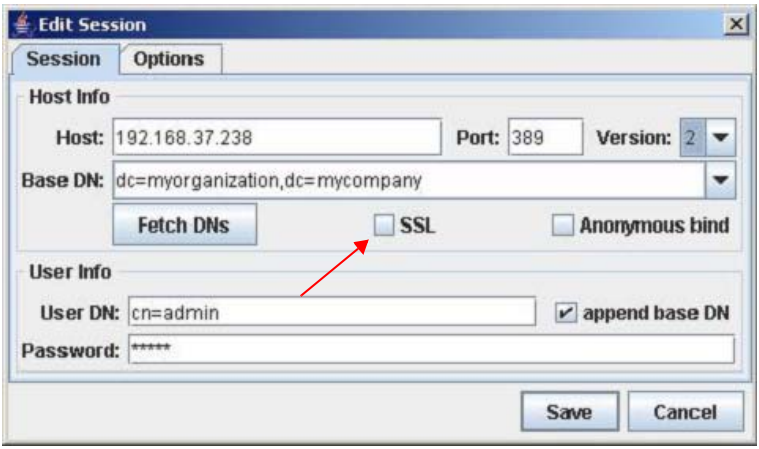


Bild 33: LDAP-Zugriff auf eDirectory testen: SSL nicht aktiviert

- Falls die Anmeldung erneut fehlschlägt:
  Lockern Sie die Bind-Restriktionen (siehe Seite 109).

4.4.5.4 iRMC-Benutzerverwaltung in Novell eDirectory integrieren

Für die Integration der iRMC-Benutzerverwaltung in Novell eDirectory sind die folgenden Schritte erforderlich:

– iRMC LDIF-Datei in eDirectory importieren.

– Principal iRMC User erzeugen.

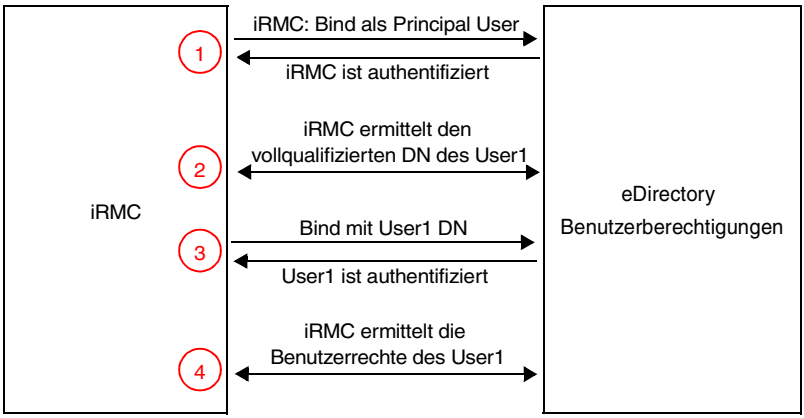
– iRMC-Gruppen und Benutzerrechte in eDirectory vereinbaren.

– Benutzer zur Organizational Unit (OU) i*RMCgroups* zuordnen.

LDAP-Authentifizierungsprozess für iRMC-Benutzer in eDirectory

Die Authentifizierung eines globalen iRMC-Benutzers beim Login am iRMC erfolgt nach einem fest vorgegebenen Schema (siehe Seite 60). Bild 34 auf Seite 113 veranschaulicht diesen Prozess für die globale iRMC-Benutzerverwaltung mithilfe von Novell eDirectory.

Das Herstellen einer Verbindung und die Anmeldung mit entsprechenden Anmeldeinformationen wird als BIND-Operation bezeichnet.



1) Der iRMC loggt sich am eDirectory-Server mit vordefinierten, bekannten Berechtigungsdaten (iRMC-Einstellung) als „Principal User“ ein und wartet auf den erfolgreichen Bind.

2) Der iRMC erfragt vom eDirectory-Server den voll-qualifizierten Distinguished Name (DN) des Benutzers mit „cn=User1“. eDirectory ermittelt den DN aus dem vorkonfigurierten Teilbaum (iRMC-Einstellung).

3) Der iRMC loggt sich am eDirectory-Server mit dem vollqualifizierten DN des Benutzers User1 ein und wartet auf den erfolgreichen Bind.

4) Der iRMC erfragt vom eDirectory-Server die Benutzerberechtigungen des Benutzers User1.

Bild 34: Authentifizierungschema für globale iRMC-Benutzerberechtigungen

Die Berechtigungsdaten des „Principal User“ sowie den Teilbaum, der die DNs enthält, konfigurieren Sie in der Seite *Directory Service Configuration* der iRMC-Web-Oberfläche (siehe Seite 273).

Der CN eines Benutzers muss innerhalb des durchsuchten Teilbaums eindeutig sein.

LDIF-Datei in Novell eDirectory importieren

Voraussetzung:

LDIF-Datei ist erstellt (siehe Abschnitt „Struktur „iRMCgroups“ im LDAP Directory Service generieren“ auf Seite 76).

Für den Import der iRMC-LDIF-Datei in Novell eDirectory verwenden Sie den iManager.

Gehen Sie wie folgt vor:

- Starten Sie den iManager via Web-Browser.
- Loggen Sie sich beim iManager mit gültigen Authentisierungsdaten ein.
- Wählen Sie *eDirectory Maintenance* und verwenden Sie den ICE (Import Convert Wizard).
- Wählen Sie *Import data from file on disk* und klicken Sie auf *Next*.
- Navigieren Sie im Datei-Browser zu Ihrer LDIF-Datei.
- Deaktivieren Sie die Option *exit on error* und klicken Sie auf *Next.*
- Geben Sie die den DNS-Namen / die IP-Adresse Ihres LDAP-Servers ein sowie die Berechtigungsdaten der Administrationskennung (siehe Bild 35 auf Seite 115).

  Verwenden Sie für den Import der LDIF-Datei eine SSL-Verbindung (Port 636).

  Verwenden Sie für den Import der LDIF-Datei die Version 2 des LDAP-Protokolls.

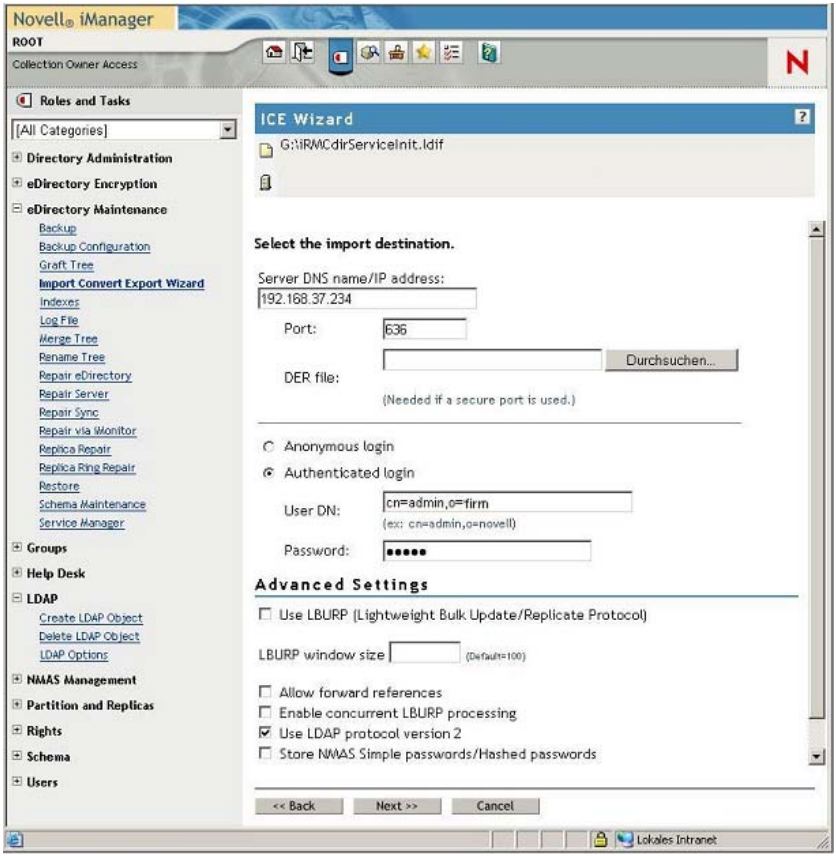


Bild 35: iManager - Roles and Tasks ICE Wizard

- Klicken Sie auf *Next*.
- Klicken Sie auf *Finish*, um den Import der LDIF-Datei zu starten.

Principal User für den iRMC erzeugen

Um einen Principal User für den iRMC zu erzeugen, gehen Sie wie folgt vor:

- Loggen Sie sich mit gültigen Authentisierungsdaten beim iManager ein.
- Wählen Sie *Roles and Tasks*.
- Wählen Sie *Users - Create User*.
- Tragen Sie die erforderlichen Angaben in das angezeigte Template ein.

  Distinguished Name (DN) und Passwort des Principal Users müssen mit entsprechenden Angaben für die Konfiguration des iRMC übereinstimmen (siehe Abschnitt „Directory Service Configuration (LDAP) - Directory Service am iRMC konfigurieren“ auf Seite 273).

  Der *Context:* des Benutzers kann sich an beliebiger Stelle im Baum befinden.

- Erteilen Sie dem Principal User Suchberechtigung für die folgenden Teilbäume:
  - Teilbaum (OU) *iRMCgroups*
  - Teilbaum (OU), der die Benutzer enthält (z.B. *people*).

Den iRMC-Gruppen und -Benutzern Benutzerrechte erteilen

Standardmäßig verfügt ein Objekt in eDirectory nur über sehr eingeschränkte Abfrage- und Suchberechtigungen in einem LDAP-Baum. Damit ein Objekt alle Attribute in einem oder mehreren Teilbäumen abfragen kann, müsse Sie diesem Objekt die entsprechenden Rechte zuweisen.

Berechtigungen erteilen Sie wahlweise einem einzelnen Objekt (d.h. einem speziellen Benutzer) oder einer Gruppe von Objekten, die in einer Organizational Unit (OU) wie z.B. *iRMCgroups* oder *people* zusammengefasst sind. Dabei gehen Berechtigungen, die einer OU erteilt und als „inherited“ gekennzeichnet sind, automatisch auf die Objekte dieser Gruppe über.

Für die Integration der iRMC-Benutzerverwaltung in Novell eDirectory ist es erforderlich, folgenden Objekten (Trustees) Suchberechtigung zu erteilen:

- *Principal User*
- Teilbaum, der die iRMC-Benutzer enthält

Wie Sie dabei im Einzelnen vorgehen ist nachfolgend beschrieben.

Um einem Objekt die Suchberechtigung für alle Attribute zu erteilen, verfahren Sie wie folgt:

- Starten Sie den iManager via Web-Browser.
- Loggen Sie sich beim iManager mit gültigen Authentisierungsdaten ein.
- Klicken Sie im iManager auf die Schaltfläche *Roles and Tasks*.
- Wählen Sie im Menübaum *Rights - Rights to Other Objects*.

  Die Seite *Rights to Other Objects* wird angezeigt.
- Spezifizieren Sie unter *Trustee Name* den Namen des Objekts (im Beispiel: *iRMCgroups.sbrd4*), dem die Berechtigung erteilt werden soll.
- Spezifizieren Sie unter *Context to Search From* den eDirectory-Teilbaum (*iRMCgroups*), den der iManager nach allen Objekten durchsuchen soll, für die der Trustee *Users* zurzeit leseberechtigt ist.
- Klicken Sie auf die Schaltfläche *OK*.

  Eine Fortschrittanzeige informiert über den Stand der Suche. Nach Abschluss des Suchvorgangs wird die Seite *Rights to Other Objects* angezeigt, die jetzt das Suchergebnis enthält (siehe Bild 36 auf Seite 118).

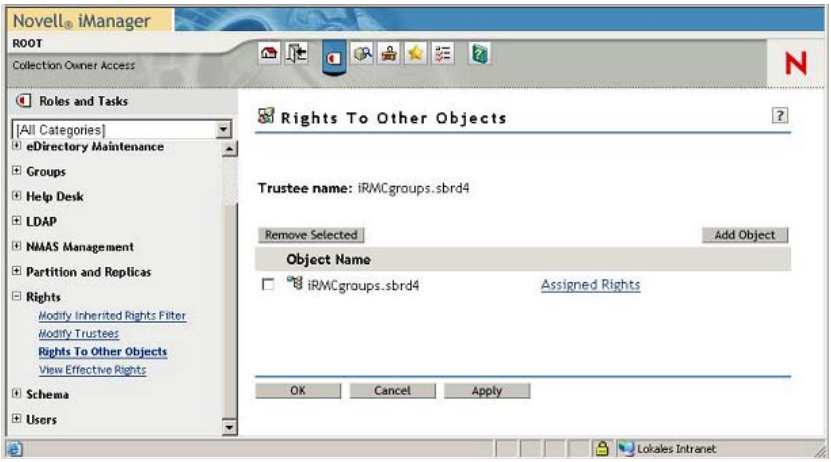


Bild 36: iManager - Roles and Tasks - Rights To Other Objects

Falls unter *Object Name* kein Objekt angezeigt wird, hat der Trustee zurzeit keine Berechtigung innerhalb des angegebenen Kontexts.

► Erteilen Sie dem Trustee gegebenenfalls zusätzliche Berechtigung(en):

► Klicken Sie auf *Add Object*.

► Selektieren Sie via Objektselektor-Schaltfläche das Objekt, für das Sie dem Trustee eine Berechtigung erteilen wollen.

► Klicken Sie auf *Assigned Rights*.

Falls die Property *[All Attributes Rights]* nicht angezeigt wird:

► Klicken Sie auf *Add Property*.

Das *Add Property*-Fenster wird angezeigt (siehe Bild 37 auf Seite 119).

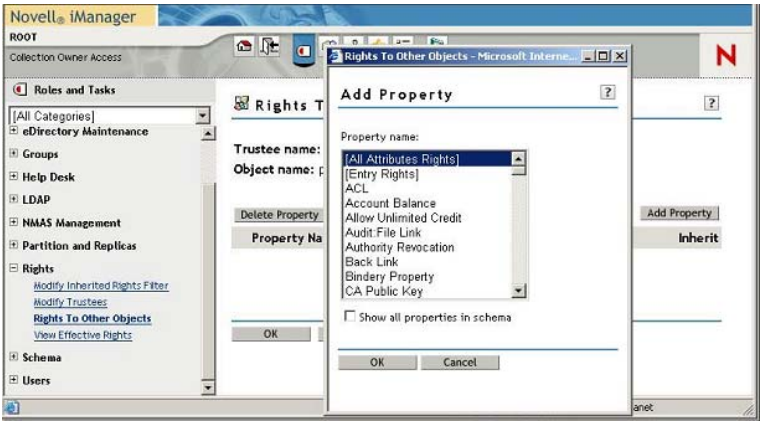


Bild 37: iManager - Roles and Tasks - Rights To Other Objects - Add Property

► Markieren Sie die Property *[All Attributes Rights]* und fügen Sie durch Klicken auf *OK* hinzu.

► Aktivieren Sie für die Property *[All Attributes Rights]* die Optionen *Compare*, *Read* und *Inherit* und bestätigen Sie mit *OK*.

Damit sind Benutzer/Benutzergruppe zur Abfrage aller Attribute im Teilbaum des ausgewählten Objekts autorisiert.

► Klicken Sie auf *Apply*, um Ihre Einstellungen zu aktivieren.

4.4.5.5 iRMC-Benutzer der OU „iRMCgroups“ zuordnen

Die Zuordnung von iRMC-Benutzern z.B. der OU *people* zur OU *iRMCgroups* können Sie wahlweise vornehmen

– ausgehend von den einzelnen Benutzereinträgen (günstig bei wenigen Benutzereinträgen) oder

– ausgehend vom Gruppeneintrag (günstig bei vielen Benutzereinträgen).

Nachfolgend ist exemplarisch die Zuordnung von iRMC-Benutzern einer OU *people* zur OU *iRMCgroups* dargestellt. Erläutert wird dabei die vom Gruppeneintrag ausgehende Zuordnung. Eine Zuordnung, die von den Benutzereinträgen ausgeht, verläuft weitgehend analog.

Gehen Sie wie folgt vor:

► Starten Sie den iManager via Web-Browser.

► Loggen Sie sich beim iManager mit gültigen Authentisierungsdaten ein.

► Wählen Sie *Roles and Tasks*.

► Wählen Sie *Groups - Modify Group*.

Die Seite *Modify Group* wird angezeigt.

► Führen Sie die folgenden Schritte für alle iRMC-Gruppen durch, denen Sie iRMC-Benutzer zuordnen wollen:

► Selektieren Sie via Objektselektor-Schaltfläche die iRMC-Gruppe, der Sie iRMC-Benutzer hinzufügen wollen.
(Im Beispiel ist dies *Administrator.Others.Departments.iRMCgroups.sbrd4*.)

► Wählen Sie die Registerkarte *Members*.

Die Registerkarte *Members* der Seite *Modify Group* wird angezeigt:

Bild 38: iManager - Roles and Tasks - Modify Group - Registerkarte „Members“

► Führen Sie den folgenden Schritt für alle Benutzer der OU *people* durch, die Sie der ausgewählten iRMC-Gruppe zuordnen wollen:

  ► Klicken Sie auf die Objektselektor-Schaltfläche .

  Das *Object Selector (Browser)*-Fenster wird geöffnet:

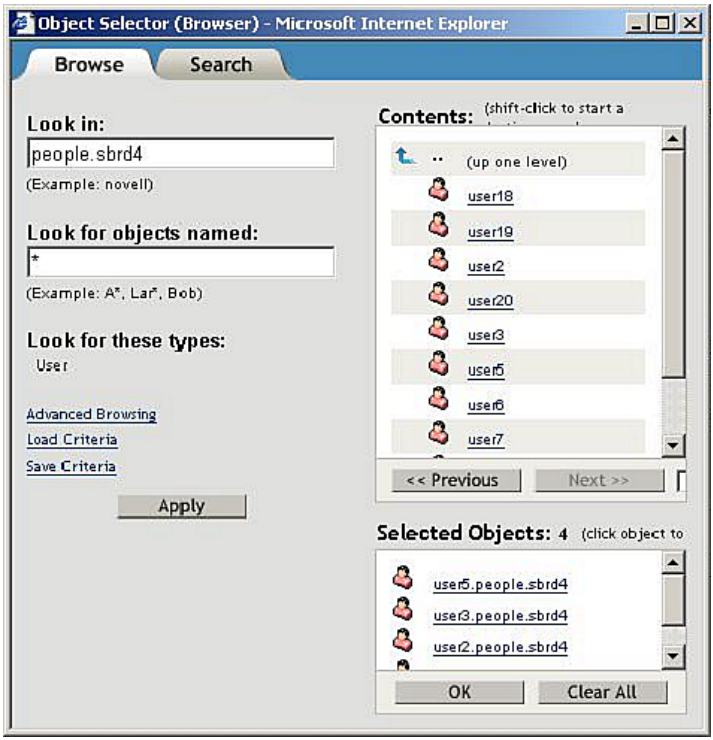


Bild 39: Benutzer der iRMC-Gruppe zuordnen - Benutzer auswählen

► Selektieren Sie im *Object Selector (Browser)*-Fenster den/die gewünschten Benutzer der OU *people* und bestätigen Sie Ihre Auswahl mit *OK*.

Im Anzeigebereich der Registerkarte *Members* der Seite *Modify Group* werden die ausgewählten Benutzer angezeigt (siehe Bild 40 auf Seite 123).

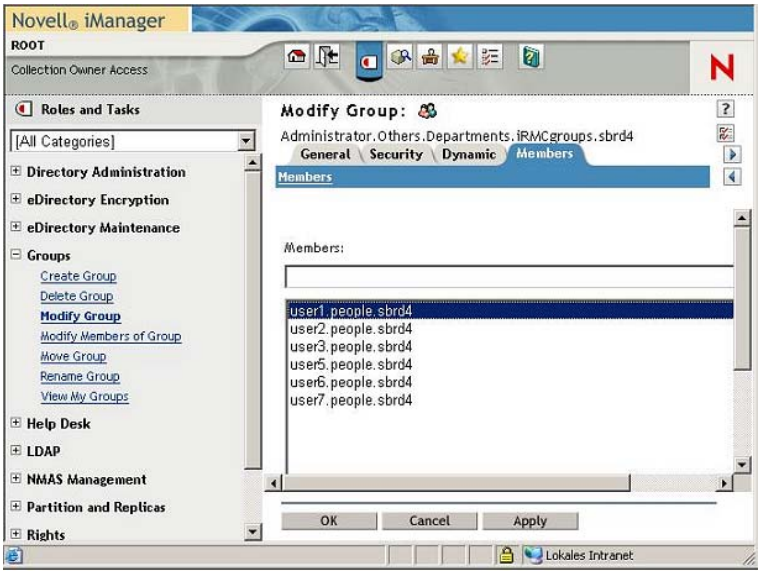


Bild 40: Anzeige der ausgewählten iRMC-Benutzer in der Registerkarte „Members

► Bestätigen Sie mit *Apply* oder *OK*, um die ausgewählten Benutzer zur iRMC-Gruppe (hier: *... .iRMCgroups.sbdr4*) hinzuzufügen.

4.4.5.6 Tipps zur Administration von Novell eDirectory

NDS-Dämon neu starten

Für einen Neustart des NDS-Dämons gehen Sie wie folgt vor:

- ► Öffnen Sie die Command Box.
- ► Melden Sie sich mit Root-Berechtigung an.
- ► Führen Sie das folgende Kommando aus:

```
rcndsd restart
```

Falls sich der lndap-Dämon ohne ersichtlichen Grund nicht starten lässt:

- ► Starten Sie den *lndap*-Dämon „von Hand“:

```
/etc/init.d/nldap restart
```

Falls der iManager nicht reagiert:

- ► Starten Sie den iManager neu:

```
/etc/init.d/novell-tomcat4 restart
```

Konfiguration des NLDAP-Servers neu laden

Gehen Sie wie folgt vor:

- ► Starten Sie ConsoleOne und loggen Sie sich in eDirectory ein.

  Wenn Sie ConsoleOne zum ersten Mal starten, ist noch kein Baum konfiguriert.

  Zur Konfiguration eines Baums gehen Sie wie folgt vor:

  - ► Wählen Sie unter *My World* den Knoten *NDS*.
  - ► Wählen Sie in der Menü-Leiste: *File - Authenticate*
  - ► Geben Sie für das Login die folgenden Authentifizierungsdaten ein:

    1. Login-Name: root
    2. Passwort: <passwort>
    3. Tree: MY_TREE
    4. Context: mycompany

- Klicken Sie links im Fenster auf das *Base DN*-Objekt (*Mycompany*).

  Auf der rechten Fensterseite wird dann das *LDAP Server*-Objekt angezeigt.

- Klicken Sie mit der rechten Maustaste auf das *LDAP Server*-Objekt und wählen Sie *Properties...* im Kontext-Menü.

- Klicken Sie in der Registerkarte *General* auf die Schaltfläche *Refresh NLDAP Server Now*.

NDS Meldungs-Trace konfigurieren

Der *nds*-Dämon erzeugt Debug-und Log-Meldungen, die Sie mit dem Tool *ndstrace* verfolgen können. Zweck der im Folgenden beschriebenen Konfiguration ist es, den Terminal-Output von *ndstrace* in eine Datei umzuleiten und sich den Inhalt dieser Datei an einem anderen Terminal anzeigen zu lassen. Für Letzteres verwenden Sie das Tool *screen*.

Es empfiehlt sich folgende Vorgehensweise:

- Öffnen Sie die Command Box (z.B. *bash*).

ndstrace konfigurieren

- Wechseln Sie in das eDirectory-Verzeichnis */home/eDirectory*:

  ```
  cd /home/eDirectory
  ```

- Starten Sie *screen* mit dem Kommando `screen`.

- Starten Sie *ndstrace* mit dem Kommando `ndstrace`.

- Selektieren Sie die Module, die Sie aktivieren wollen.

  Wollen Sie sich z.B. die Zeitpunkte anzeigen lassen wollen, an denen Ereignisse eingetreten sind, dann geben Sie `dstrace TIME` ein.

  Es wird dringend empfohlen, die Module *LDAP* und *TIME* durch zu folgende Eingabe zu aktivieren:

  ```
  dstrace LDAP TIME
  ```

- Beenden *ndstrace* durch Eingabe von *quit*.

  Damit ist die Konfiguration von *ndstrace* abgeschlossen.

Meldungsausgabe auf zweites Terminal umleiten

- Starten Sie *ndstrace* und leiten Sie die Meldungsausgebe um:

  ```
  ndstrace -l >ndstrace.log
  ```

- Öffnen Sie ein zweites Terminal mithilfe der folgenden Tastenkombination: Ctrl + a, Crtl + c
- Schalten Sie den Mitschnitt der Protokollierung ein:

  ```
  tail -f ./ndstrace.log
  ```

- Um zwischen den virtuellen Terminals hin- und herzuschalten, verwenden Sie die Tastenkombination Ctrl + a, Crtl + 0.
  (Die Terminals sind von 0 bis 9 durchnummeriert.)

4.4.6 iRMC-Benutzerverwaltung via OpenLDAP

Dieser Abschnitt informiert über die folgenden Themen:

– OpenLDAP installieren (Linux).

– SSL-Zertifikat erzeugen.

– OpenLDAP konfigurieren.

– iRMC-Benutzerverwaltung in OpenLDAP integrieren.

– Tipps zur Administration von OpenLDAP

4.4.6.1 OpenLDAP installieren

Vor der Installation von OpenLDAP müssen Sie die Firewall für Verbindungen zu den Ports 389 und 636 konfigurieren.

Bei OpenSuSE verfahren Sie hierfür wie folgt:

► Ergänzen Sie in der Datei */etc/sysconfig/SuSEfirewall2* die Option *FW_SERVICES_EXT_TCP* wie folgt:

```
FW_SERVICES_EXT_TCP="389 636"
```

Zur Installation der Packages *OpenSSL* und *OpenLDAP2* vom Distributionsmedium verwenden Sie das Setup-Tool YaST.

4.4.6.2 SSL-Zertifikate erzeugen

Es soll ein Zertifikat mit folgenden Eigenschaften erzeugt werden:

– Schlüssellänge: 1024 bit
– md5RSAEnc

Schlüsselpaare und signierte Zertifikate (selbstsigniert oder von einer externen CA signiert) erzeugen Sie mithilfe von OpenSSL. Nähere Informationen hierzu finden Sie auf der OpenSSL-Homepage unter *http://www.openssl.org*.

Unter den folgenden Links finden Sie Anleitungen zur Einrichtung einer CA und zum Erstellen von Test-Zertifikaten:

– *http://www.akadia.com/services/ssh_test_certificate.html*
– *http://www.freebsdmadeeasy.com/tutorials/web-server/apache-ssl-certs.php*
– *http://www.flatmtn.com/computer/Linux-SSLCertificates.html*
– *http://www.tc.umn.edu/~brams006/selfsign.html*

Als Ergebnis der Zertifikatserstellung müssen die folgenden drei PEM-Dateien vorliegen:

– Root-Zertifikat: *root.cer.pem*

– Server-Zertifikat: *server.cer.pem*

– Private Key: *server.key.pem*

Der Private Key **darf nicht** mit einer Passphrase verschlüsselt sein, da Sie **nur dem LDAP-Dämon** (*ldap*) Leseberechtigung für die Datei *server.key.pem* erteilen sollten.

Die Passphrase entfernen Sie mit folgendem Kommando:

```
openssl rsa –in server.enc.key.pem –out server.key.pem
```

4.4.6.3 OpenLDAP konfigurieren

Zur Konfiguration von OpenLDAP gehen Sie wie folgt vor:

- Starten Sie das Setup-Tool Yast und wählen Sie *LDAP-Server-Configuration*.
- Aktivieren Sie unter *Global Settings/Allow Settings* die Einstellung *LDAPv2-Bind*.
- Wählen Sie *Global Settings/TLS Settings*:
  - Aktivieren Sie die Einstellung *TLS*.
  - Geben Sie die Pfade der bei der Installation erstellten Dateien bekannt (siehe Abschnitt „OpenLDAP installieren“ auf Seite 127).
  - Stellen Sie sicher, dass Zertifikate und Privater Schlüssel im Dateisystem vom LDAP-Service gelesen werden können.

    Da *openldap* unter der *uid/guid=ldap* ausgeführt wird, können Sie dies z.B. erreichen, indem Sie

    – den Eigentümer der Dateien mit Zertifikaten und privaten Schlüsseln auf „ldap“ setzen oder

    – dem LDAP-Dämon *ldap* die Leseberechtigung auf die Dateien mit Zertifikaten und privaten Schlüsseln erteilen.
- Wählen Sie *Databases*, um eine neue Datenbank zu erzeugen.

Falls die von YaST erstellte Konfiguration generell nicht funktioniert, prüfen Sie die Konfigurationsdatei */etc/openldap/slapd.conf* auf folgende zwingend erforderlichen Einträge:

```
allow bind_v2
TLSCACertificateFile /path/to/ca-certificate.pem
TLSCertificateFile /path/to/certificate.pem
TLSCertificateKeyFile /path/to/privat.key.pem
```

Falls die von YaST erstellte Konfiguration für SSL nicht funktioniert, prüfen Sie die Konfigurationsdatei */etc/sysconfig/openldap* auf folgenden Eintrag:

```
OPENLDAP_START_LDAPS="yes"
```

4.4.6.4 iRMC-Benutzerverwaltung in OpenLDAP integrieren

Die Integration der iRMC-Benutzerverwaltung in OpenLDAP umfasst die folgenden Schritte:

– iRMC-LDIF-Datei in OpenLDAP importieren.

– Principal iRMC User erzeugen.

– Neuen iRMC-Benutzer erzeugen und der OU *iRMCgroups* zuordnen.

LDIF-Datei in OpenLDAP importieren

Voraussetzung:

LDIF-Datei ist erstellt (siehe Abschnitt „Struktur „iRMCgroups“ im LDAP Directory Service generieren“ auf Seite 76).

Für den Import der iRMC-LDIF-Datei in OpenLDAP bietet sich das Management-Tool *ldapadd* an.

Hilfe zum Tool *ldapadd* erhalten Sie durch Eingabe von

```
ldapadd --help
```

Zum Import der LDIF-Datei gehen Sie wie folgt vor:

- Kopieren Sie die LDIF-Datei auf den OpenLDAP-Server.
- Öffnen Sie auf dem OpenLDAP-Server ein Terminal.

- Wechseln Sie in das Verzeichnis, in das Sie die LDIF-Datei kopiert haben.
- Geben Sie für den Import der LDIF-Datei das folgende Kommando ein:

```
ldapadd -x -v -D „cn=admin,dc=myorganization,dc=mycompany“
        -W -f iRMCdirServiceInit.ldif
```

Principal User erzeugen

Verwenden Sie zur Erzeugung des Principal User (ObjectClass: *Person*) einen LDAP-Browser, z.B. den LDAP Browser\Editor von Jarek Gawor (siehe Seite 82).

Im Folgenden ist beschrieben, wie Sie den Principal User mithilfe des LDAP Browser\Editor von Jarek Gawor erzeugen.

Gehen Sie wie folgt vor:

- Starten Sie den LDAP Browser.
- Loggen Sie sich beim OpenLDAP Directory Service mit gültigen Authentisierungsdaten ein.
- Wählen Sie den Teilbaum (Untergruppe), in dem der Principal User angelegt werden soll. Der Principal User kann an beliebiger Stelle dieses Baums angelegt werden.
- Öffnen Sie das Menü *Edit*.
- Wählen Sie *Add Entry*.
- Wählen Sie *Person*.
- Ändern Sie den Distinguished Name *DN*.

  Distinguished Name (DN) und Passwort des Principal User müssen mit entsprechenden Angaben für die Konfiguration des iRMC übereinstimmen (siehe Abschnitt „Directory Service Configuration (LDAP) - Directory Service am iRMC konfigurieren“ auf Seite 273).
- Klicken Sie auf *Set* und geben Sie ein Passwort ein.
- Geben Sie einen Sur Name *SN* ein.
- Klicken Sie auf *Apply*.

Neuen iRMC-Benutzer erzeugen und der OU „iRMCgroups“ zuordnen

Verwenden Sie für Erzeugung eines neuen Benutzers (ObjectClass *Person*) sowie zur Zuordnung eines Benutzers zur OU *iRMCgroups* einen LDAP-Browser, z.B. den LDAP Browser\Editor von Jarek Gawor (siehe Seite 82).

Im Folgenden ist beschrieben, wie Sie mithilfe des LDAP Browser\Editor von Jarek Gawor einen neuen iRMC-Benutzer erzeugen und ihn zur OU *iRMCgroups* hinzufügen.

Gehen Sie wie folgt vor:

- Starten Sie den LDAP Browser.
- Loggen Sie sich beim OpenLDAP Directory Service mit gültigen Authentisierungsdaten ein.
- Erzeugen Sie einen neuen Benutzer:

  Gehen Sie hierbei wie folgt vor:

  - Wählen Sie den Teilbaum (Untergruppe), in dem der neue Benutzer angelegt werden soll. Der neue Benutzer kann an beliebiger Stelle des Baums angelegt werden.
  - Öffnen Sie das Menü *Edit*.
  - Wählen Sie *Add Entry*.
  - Wählen Sie *Person*.
  - Ändern Sie den Distinguished Name *DN*.
  - Klicken Sie auf *Set* und geben Sie das Passwort ein.
  - Geben Sie einen Sur Name *SN* ein.
  - Klicken Sie auf *Apply*.

- Ordnen Sie den soeben erzeugten Benutzer der OU *iRMCgroups* zu.

  Gehen Sie hierbei wie folgt vor:

  - Wählen Sie den Teilbaum (Untergruppe) von *iRMCgroups*, dem der Benutzer angehören soll, d.h. *cn=UserKVM,ou=YourDepartment, ou=Departments,ou=iRMCgroups,dc=myorganisation,dc=mycompany*
  - Öffnen Sie das Menü *Edit*.
  - Wählen Sie *Add Attribute*.
  - Geben Sie als Attributnamen „Member“ ein. Als Wert geben Sie den voll-qualifizierten DN zuvor erzeugten Benutzers an, also *cn=UserKVM,ou=YourDepartment,ou=Departments,ou=iRMCgroups, dc=myorganization,dc=mycompany*

4.4.6.5 Tipps zur Administration von OpenLDAP

LDAP-Service neu starten

Um den LDAP-Service neu zu starten, verfahren Sie wie folgt:

- Öffnen Sie die Command Box.
- Melden Sie sich mit Root-Berechtigung an.
- Geben Sie das folgende Kommando ein:

```
rcldap restart
```

Meldungsprotokollierung

Für das Meldungslogging nutzt der LDAP-Dämon das Syslog-Protokoll.

Die protokollierten Meldungen werden nur angezeigt, wenn in der Datei */etc/openldap/slapd.conf* ein Log-Level ungleich 0 eingestellt ist.

Erläuterungen zu den verschiedenen Leveln finden Sie unter:

http://www.zytrax.com/books/ldap/ch6/#loglevel

Tabelle 2 auf Seite 133 gibt einen Überblick über die Log-Level und ihre Bedeutung.

Log-Level	Bedeutung
-1	umfassendes Debugging
0	kein Debugging
1	Funktionsaufrufe protokollieren
2	Paketverarbeitung testen
4	Heavy Trace Debugging
8	Verbindungsmanagement
16	Gesendete und empfangene Pakete anzeigen
32	Suchfilterverarbeitung
64	Konfigurationsdateiverarbeitung
128	Verarbeitung der Zugangskontrolllisten
256	Status-Logging für Verbindungen / Operationen /Ergebnisse
512	Status-Logging für gesendete Einträge
1024	Kommunikation mit den Shell Backends ausgeben.
2048	Ergebnisse des Entry Parsings ausgeben.

Tabelle 2: OpenLDAP - Log-Level

4.4.7 SSL Copyright

Die iRMC-LDAP Integration verwendet die auf dem OpenSSL Project basierende SSL Implementation von Eric Young.

```
/* ====================================================================
 * Copyright (c) 1998-2002 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */
```

```
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *    the apps directory (application code) you must include an acknowledgement:
 *    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version or
 * derivative of this code cannot be changed.  i.e. this code cannot simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */
```

5 Advanced Video Redirection

Die Nutzung des Features „Advanced Video Redirection“ setzt einen gültigen License Key voraus.

Mit der Advanced Video Redirection (AVR) können Sie von Ihrem Remote-Arbeitsplatz aus Tastatur und Maus des verwalteten Servers kontrollieren und sich die aktuellen grafischen Ausgaben sowie die Text-Ausgaben des verwalteten Servers anzeigen lassen.

Über das Java-Applet der AVR können Sie das Feature Remote Storage nutzen (siehe Kapitel „Remote Storage“ auf Seite 159).

Das vorliegende Kapitel informiert über folgende Themen:

– Einstellungen für die AVR prüfen
– AVR verwenden
– Menüs des AVR-Fensters

5.1 Voraussetzungen: Die Einstellungen für die AVR überprüfen

Bevor Sie AVR nutzen, prüfen Sie folgende wichtige Einstellungen:

Einstellungen für den Grafikmodus am verwalteten Server

Advanced Video Redirection (AVR) unterstützt die folgenden Grafikmodi:

Auflösung	Wiederholungs-raten [in Hz]	maximale Farbtiefe [bit]
640 x 480 (VGA)	60; 75	32
800 x 600 (SVGA)	56; 60; 72; 75	16
1024 x 768 (XGA)	60; 70; 75	16
1152 x 864	60; 70; 75	8
1280 x 1024 (UXGA)	60; 70; 75	8

Tabelle 3: Unterstützte Einstellungen für die Bildanzeige

Es werden ausschließlich VESA-konforme Grafikmodi unterstützt.

Unterstützter Text-Modus

Der iRMC unterstützt die folgenden gebräuchlichen Text-Modi:

- 40 x 25
- 80 x 25
- 80 x 43
- 80 x 50

Für Informationen zu den Einstellungen für die Bildanzeige siehe die Hilfe zum Betriebssystem.

Tastatur-Einstellungen

Die Einstellungen für die Tastatur müssen identisch sein:

- am Remote-Arbeitsplatz
- am verwalteten Server
- am iRMC

5.2 Advanced Video Redirection verwenden

- Um die AVR zu starten, klicken Sie in der Seite *Advanced Video Redirection* der iRMC-Web-Oberfläche auf die Schaltfläche *Start Video Redirection* (siehe Seite 292).

  Es wird dann das Fenster *Advanced Video Redirection* (AVR-Fenster) geöffnet, das die Bildschirmausgabe am verwalteten Server darstellt.

  Zusätzlich enthält das AVR-Fenster folgende Elemente:

  – Menüleiste: Über die Menüs *Preferences* und *Extras* können sie die Einstellungen der AVR konfigurieren und die AVR steuern (siehe Seite 151). Über *Remote Storage* rufen Sie Remote Storage auf (siehe Seite 155).

  – Integrierte Sondertasten (siehe Seite 142).

  – Die *Local Monitor*-Anzeige informiert, ob der lokale Monitor des verwalteten Servers eingeschaltet ist (siehe Abschnitt „Local Monitor Off-Funktionalität“ auf Seite 141).

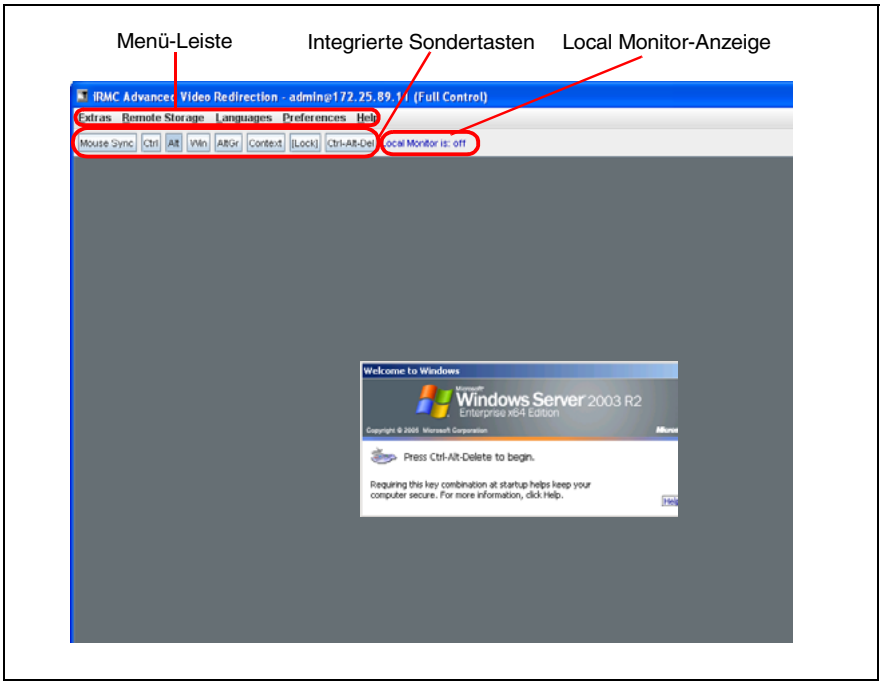


Bild 41: Fenster Advanced Video Redirection

5.2.1 Parallele AVR-Sitzungen

AVR kann von zwei Benutzer-Sitzungen gleichzeitig verwendet werden. Dabei hat einer der Benutzer die volle Kontrolle über den Server (Full Control-Modus), während der andere Benutzer die Bedienung des Servers via Tastatur- und Mauseingaben nur passiv verfolgen kann (View Only-Modus).

Nach dem Start der AVR befinden Sie sich zunächst im View Only-Modus. Sie werden in jedem Fall gefragt, ob Sie in den Full Control-Modus wechseln wollen. Falls Sie sich für den Full Control-Modus entscheiden und es ist bereits eine andere AVR-Sitzung im Full Control-Modus aktiv, wird die bereits bestehende Sitzung in den View Only-Modus versetzt.

5.2.2 Local Monitor Off-Funktionalität

Die Local Monitor Off-Funktionalität des iRMC bietet Ihnen die Möglichkeit, den lokalen Monitor des verwalteten Servers für die Dauer Ihrer AVR-Sitzung auszuschalten. Auf diese Weise stellen Sie sicher, dass am lokalen Monitor des Servers Ihre via AVR durchgeführten Eingaben und Aktionen nicht sichtbar sind. Am Server wird „Local Monitor Off“ durch Blinken der Identifizierungs-LED signalisiert.

Die Local Monitor Off-Funktionalität wird nicht von allen PRIMERGY-Servern mit iRMC unterstützt.

Die Local Monitor Off-Funktionalität konfigurieren Sie über die Seite *Advanced Video Redirection* der iRMC-Web-Oberfläche (siehe Seite 292). Nach entsprechender Konfiguration können Sie den lokalen Monitor des Servers vom Remote-Arbeitsplatz aus wie folgt an- und ausschalten:

– im Full Control-Modus einer AVR-Sitzung über das Menü *Extras*

– mit Administrator- oder OEM-Berechtigung direkt auf der Seite *Advanced Video Redirection*

Zusätzlich können Sie konfigurieren, dass sich der lokale Monitor beim Start einer neuen AVR-Sitzung immer automatisch ausschaltet.

Der aktuelle Status des lokalen Monitors wird im AVR-Fenster rechts neben den integrierten Sondertasten als blauer Schriftzug angezeigt:

Local Monitor always on
: Der lokale Monitor ist immer eingeschaltet und kann nicht ausgeschaltet werden, da die Option *Enable Local Monitor Off* (siehe Seite 294) deaktiviert ist.

Local Monitor is: on
: Der lokale Monitor ist eingeschaltet, kann aber ausgeschaltet werden.

Local Monitor is: off
: Der lokale Monitor ist ausgeschaltet, kann aber eingeschaltet werden.

5.2.3 Umleitung der Tastatur

Die Tastatur-Umleitung funktioniert nur, wenn das AVR-Fenster den Eingabe-Fokus hat:

- Falls die Tastatur-Umleitung nicht zu funktionieren scheint, klicken Sie einfach auf das AVR-Fenster.
- Falls die Tastatur nicht reagiert, überprüfen Sie, ob sich das AVR-Fenster im View Only-Modus befindet. Wie Sie in den Full Control-Modus umschalten, ist auf Seite 153 beschrieben.

Besondere Tastenkombinationen

AVR überträgt alle normalen Tastenkombinationen an den Server. Sondertasten, wie z.B. Windows-Tasten, werden nicht übertragen. Einige spezielle Tastenkombinationen, wie z.B. ALT + F4, können nicht übertragen werden, da sie vom Betriebssystem des Client abgefangen werden. In diesen Fällen behelfen Sie sich mit den integrierten Sondertasten oder der virtuellen Tastatur.

Integrierte Sondertasten

Unterhalb der Menüleiste finden Sie im AVR-Fenster die Leiste mit den Sondertasten. Diese Tasten sind als „Sticky Key“ implementiert, d.h. sie bleiben nach Anklicken „gedrückt“ und werden erst durch erneutes Anklicken in die Grundstellung zurückgesetzt.

Mithilfe der integrierten Sondertasten können Sie z.B. Windows-Tasten oder spezielle Tastenkombinationen nutzen, die bei Eingabe über Ihre Tastatur nicht via AVR übertragen werden können.

Bild 42: Fenster Advanced Video Redirection - Integrierte Sondertasten

Mouse Sync
: Durch Drücken dieser Taste synchronisieren Sie die Mauszeiger (siehe auch Abschnitt „Mauszeiger synchronisieren“ auf Seite 144).

Ctrl
: Linke Kontrolltaste (entspricht der Taste Strg (Ctrl) auf Ihrer Tastatur).

Alt
: Alt(ernate)-Taste (entspricht der Taste Alt auf Ihrer Tastatur).

Win

Linke und rechte Windows-Taste (entsprechen auf Ihrer Tastatur den Tasten Strg und Alt bzw. Alt Gr und Strg).

Alt Gr

Alt(ernate) Gr(aphic)-Taste (entspricht der Taste Alt Gr auf Ihrer Tastatur).

Context

Kontext-Menü für das markierte Objekt (entspricht der Tastenkombination Shift + F10 auf Ihrer Tastatur).

Lock

Feststelltaste (entspricht der Taste Caps Lock auf Ihrer Tastatur).

Ctrl-Alt-Del

Entspricht der Tastenkombination Strg + Alt + Del auf Ihrer Tastatur.

Virtual Keyboard (virtuelle Tastatur)

Die „virtuelle Tastatur“ (siehe Bild 43) bietet Ihnen eine bedienbare Abbildung der Tastatur. Bei Verwendung der virtuellen Tastatur stehen Ihnen alle Tastenkombination zur Verfügung. Somit können Sie die virtuelle Tastatur als vollwertige Alternative für eine reale Tastatur bedienen.

Die „virtuelle Tastatur“ aktivieren Sie im AVR-Fenster über das Menü *Extras* (siehe Seite 152).

Bild 43: Virtual Keyboard (Tastatur-Layout: German (DE))

Secure Keyboard

Wenn Sie über eine HTTPS-Verbindung mit der iRMC-Web-Oberfläche verbunden sind, werden die Tastatureingaben SSL-gesichert übertragen.

5.2.4 Umleitung der Maus

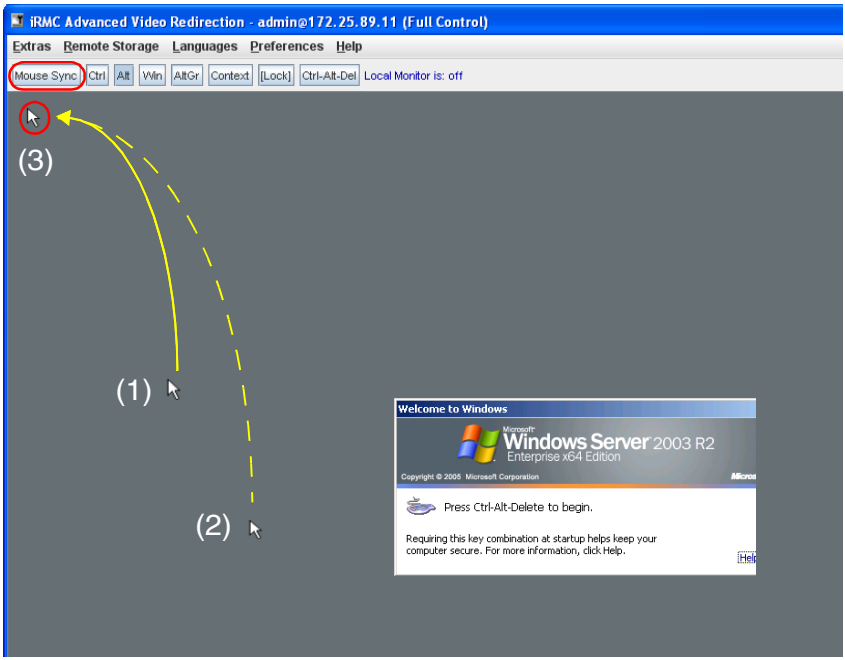
Der Mauszeiger des verwalteten Servers wird synchron mit der Maus am Remote-Arbeitsplatz bewegt. Die Einstellungen für die Umleitung der Maus konfigurieren Sie im AVR-Fenster über das Menü *Preferences* - Registerkarte *Mouse* (siehe Seite 156).

5.2.4.1 Mauszeiger synchronisieren

Möglicherweise ist nach dem Öffnen des AVR-Fensters der Mauszeiger am Remote-Arbeitsplatz (lokaler Mauszeiger) noch nicht mit dem Mauszeiger am verwalteten Server synchronisiert.

Um beide Mauszeiger zu synchronisieren, verfahren Sie wahlweise nach einer der beiden folgenden Alternativen (siehe Bild 44 auf Seite 145):

- Drücken Sie in der Menü-Leiste des AVR-Fensters die Taste Mouse Sync.
- Ziehen Sie den lokalen Mauszeiger in die linke obere Ecke des AVR-Fensters. Der Mauszeiger des verwalteten Servers folgt automatisch. Sobald sich beide Mauszeiger vollständig überlappen, sind die Zeiger synchronisiert.


iRMC Advanced Video Redirection - admin@172.25.89.11 (Full Control)
Extras Remote Storage Languages Preferences Help
Mouse Sync Ctrl Alt Win AltGr Context [Lock] Ctrl-Alt-Del Local Monitor is: off
(3)
(1)
(2)
Welcome to Windows
Windows Server 2003 R2
Enterprise x64 Edition
Press Ctrl-Alt-Delete to begin.
Requiring this key combination at startup helps keep your computer secure. For more information, click Help.

Mouse Sync -Taste drücken

oder

(1) Lokalen Mauszeiger in die linke obere Ecke ziehen.

(2) Mauszeiger des Servers folgt automatisch.

(3) Die Mauszeiger sind synchronisiert, wenn sie sich vollständig überlappen und im AVR-Fenster als **ein** Mauszeiger dargestellt werden.

Bild 44: Lokalen Mauszeiger und Mauszeiger des verwalteten Servers synchronisieren.

Die einwandfreie Synchronisation der Mauszeiger erfordert bestimmte Einstellungen am verwalteten Server, die durch die Matrox VGA Treiber-Installation auf dem verwalteten Server automatisch vorkonfiguriert werden.

Wenn die Synchronisation der Mauszeiger nicht optimal funktioniert, z.B. weil die vorkonfigurierten Einstellungen verändert wurden, können Sie mit den im Folgenden beschriebenen Einstellungen die einwandfreie Synchronisation der Mauszeiger wiederherstellen. Diese Einstellungen sind für den verwalteten Server vorzunehmen.

5.2.4.2 Verwalteter Windows Server: Einstellungen für Mauszeiger-Synchronisation anpassen

Für einen Windows Server können Sie die Einstellungen für die Mauszeiger-Synchronisation wahlweise via Batch-Programm oder über das Windows Startmenü und Kontext-Menü modifizieren.

Folgende Einstellungen müssen Sie anpassen:

– Geschwindigkeit des Mauszeigers
– Hardwarebeschleunigung

Wenn Sie die Einstellungen via Batch-Programm anpassen, wird zusätzlich zur Anpassung von Mauszeiger-Geschwindigkeit und Hardwarebeschleunigung der Matrox Grafik-Treiber installiert.

Alle Einstellungen für den verwalteten Server können Sie wahlweise direkt am verwalteten Server oder via AVR vom Remote-Arbeitsplatz aus vornehmen.

Einstellungen am verwalteten Server via Batch-Programm anpassen

Gehen Sie wie folgt vor:

- Öffnen Sie die Windows-Eingabeaufforderung.
- Wechseln Sie in das Verzeichnis, in dem das Batch-Programm *ServerEnginesG200e_Kronos1_SETUP.exe* der jeweiligen Matrox VGA Treiber-Installation (32 Bit oder 64 Bit) gespeichert ist.
- Geben Sie *setup.bat* ein und starten Sie das Batch-Programm.
- Starten Sie nach Ausführung des Batch-Programms den verwalteten Server neu.

Einstellungen am verwalteten Server über Windows Start- und Kontext-Menü anpassen

Zur Anpassung des Mauszeigers gehen Sie wie folgt vor:

► Wählen Sie

Start - Einstellungen - Systemsteuerung - Drucker und andere Hardware - Maus - Registerkarte *Zeigeroptionen*.

Das folgende Fenster wird angezeigt:

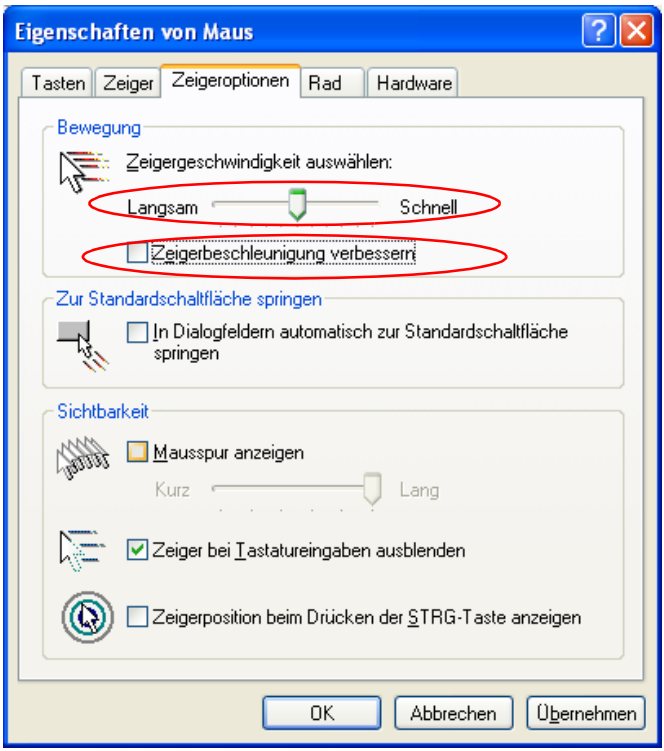


Bild 45: Eigenschaften von Maus - Zeigeroptionen

► Setzen Sie die *Zeigergeschwindigkeit* auf einen mittleren Wert.

► Deaktivieren Sie die Option *Zeigerbeschleunigung verbessern*.

► Klicken Sie auf die Schaltfläche OK, um die Einstellungen zu sichern.

Zur Anpassung der Hardwarebeschleunigung gehen Sie wie folgt vor:

- ► Klicken Sie mit der rechten Maustaste auf den Hintergrund.
- ► Wählen Sie im Kontextmenü:

  Eigenschaften - Registerkarte *Einstellungen* - Schaltfläche *Erweitert* - Registerkarte *Problembehandlung*.

  Das folgende Fenster wird angezeigt:

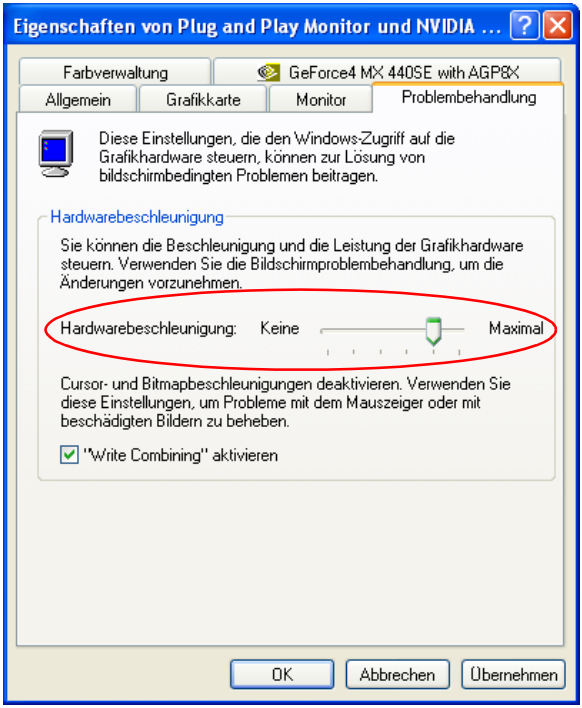

Eigenschaften von Plug and Play Monitor und NVIDIA ...
Farbverwaltung
GeForce4 MX 440SE with AGP8X
Allgemein
Grafikkarte
Monitor
Problembehandlung
Diese Einstellungen, die den Windows-Zugriff auf die Grafikhardware steuern, können zur Lösung von bildschirmbedingten Problemen beitragen.
Hardwarebeschleunigung
Sie können die Beschleunigung und die Leistung der Grafikhardware steuern. Verwenden Sie die Bildschirmproblembehandlung, um die Änderungen vorzunehmen.
Hardwarebeschleunigung: Keine Maximal
Cursor- und Bitmapbeschleunigungen deaktivieren. Verwenden Sie diese Einstellungen, um Probleme mit dem Mauszeiger oder mit beschädigten Bildern zu beheben.
"Write Combining" aktivieren
OK
Abbrechen
Übernehmen

Bild 46: Eigenschaften - ... - Problembehandlung: Hardwarebeschleunigung

- ► Setzen Sie die *Hardwarebeschleunigung* auf einen Wert wie in Bild 46.
- ► Klicken Sie auf die Schaltfläche OK, um die Einstellungen zu sichern.

5.2.4.3 Verwalteter Linux Server: Einstellungen für Mauszeiger-Synchronisation anpassen

Voraussetzung: Der verwaltete Server läuft unter einem der folgenden Linux-Betriebssysteme:

- Red Hat 4.x
- Red Hat 5.x
- Suse 9.x
- Suse 10.x

Die Einstellungen für die Mauszeiger-Synchronisation können Sie auf dem verwalteten Server wahlweise per Kommando oder Menü-geführt anpassen.

Folgende Einstellungen müssen Sie anpassen:

- *Pointer acceleration*
- *Pointer threshold*

Alle Einstellungen für den verwalteten Server können Sie wahlweise direkt am verwalteten Server oder via AVR vom Remote-Arbeitsplatz aus vornehmen.

Einstellungen am verwalteten Server via Kommando anpassen

Mit dem Kommando *xset* setzen Sie die Einstellungen für *Pointer acceleration* und *Pointer threshold* (empfohlene Werte: jeweils 1).

Kommando-Syntax:

`xset m(ouse)[`*acceleration*`][`*threshold*`]`

Gehen Sie wie folgt vor:

- ▶ Rufen Sie ein Kommandozeilen-Tool auf.
- ▶ Führen Sie das Kommando *xset* mit folgenden Argumenten aus:

```
xset m 1 1
```

Einstellungen am verwalteten Server Menü-geführt anpassen

Das im Folgenden beschriebene Verfahren gilt nur für Suse Linux.

Gehen Sie wie folgt vor:

- Wählen Sie

  N - Control Center - Periferal - Mouse - Registerkarte *Advance*

  Das Fenster *Mouse - Control Center* wird angezeigt:

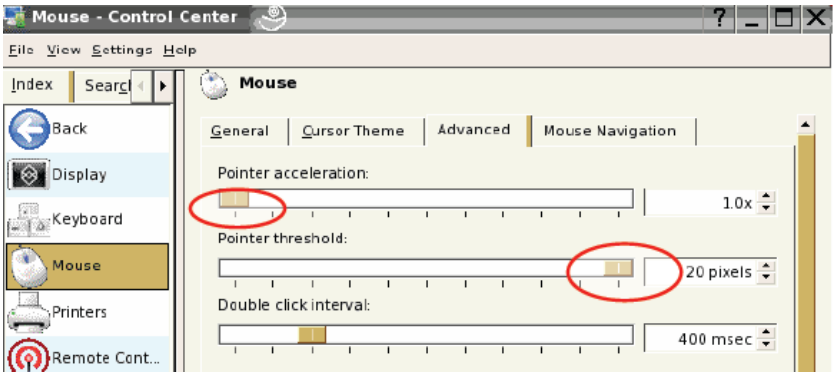


Bild 47: Fenster Mouse Control Center Window

- Setzen Sie im Fenster *Mouse Control Center Window* folgende Werte:
  - *Pointer acceleration:* 1.0x (Minimalwert)
  - *Pointer threshold:* 20 Pixel (Maximalwert)
- Sichern Sie die Einstellungen.
- Starten Sie den verwalteten Server neu.

  Ein erneutes Setzen der Werte nach dem Neustart des Servers ist nicht erforderlich.

5.3 Menüs des AVR-Fensters

Die Menü-Leiste des Fensters *Advanced Video Redirection* enthält folgende Menüs:

– Über das Menü *Extras* steuern Sie die AVR-Sitzung. Außerdem können Sie eine virtuelle Tastatur bereitstellen.

– Über das Menü *Remote Storage* können Sie Remote Storage Verbindungen herstellen und trennen.

– Über das Menü *Languages* wählen Sie die Landessprache (Deutsch/Englisch), in der die AVR-Menüs und -Dialoge angezeigt werden.

– Über das Menü *Preferences* konfigurieren Sie die Einstellungen für Maus, Tastatur und Logging.

5.3.1 Menü Extras

Im Menü *Extras* können Sie zwischen folgenden Funktionen wählen:

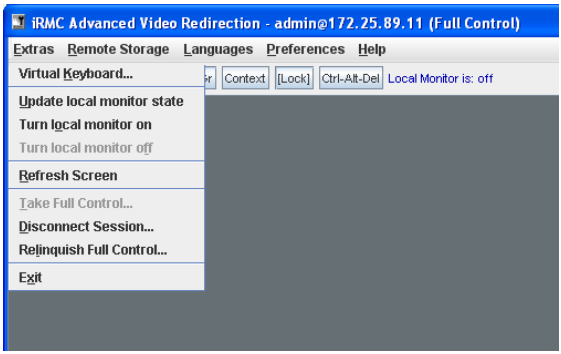


Bild 48: Fenster der Advanced Video Redirection - Menü Extras

Virtual Keyboard ...

Das Fenster *Virtual Keyboard* (virtuelle Tastatur) öffnet sich (siehe Bild 43 auf Seite 143).

Update local monitor state

Local Monitor-Anzeige aktualisieren.

Turn local monitor on

Diese Funktion wird nicht von allen PRIMERGY-Servern unterstützt.

Lokalen Monitor des verwalteten Servers einschalten.

Wenn Sie sich im View-only-Modus befinden, ist die Funktion auch bei ausgeschaltetem lokalen Monitor deaktiviert.

Turn local monitor off

Diese Funktion wird nicht von allen PRIMERGY-Servern unterstützt.

Lokalen Monitor des verwalteten Servers ausschalten.

Auch wenn der lokale Monitor eingeschaltet ist, ist die Funktion in folgenden Fällen deaktiviert:

– Sie befinden sich im View-only-Modus.

– Beim Start der AVR war unter *Local Monitor* die Option *Enable Local Monitor Off* nicht aktiviert (siehe Seite 294). Local Monitor-Anzeige: *Local Monitor always on*

Refresh Screen

AVR-Fenster aktualisieren.

Take Full Control...

In den Full Control-Modus wechseln. (Falls Sie sich bereits im Full Control-Modus befinden, ist diese Funktion deaktiviert.)

Das folgende Dialogfenster wird geöffnet:

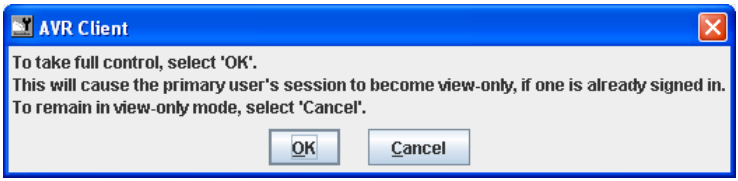

AVR Client
To take full control, select 'OK'.
This will cause the primary user's session to become view-only, if one is already signed in.
To remain in view-only mode, select 'Cancel'.
OK
Cancel

Bild 49: Menü Extras - Take Full Control...

► Bestätigen Sie mit *OK*, wenn Sie in den Full Control-Modus wechsel wollen.

Beachten Sie, dass hierdurch eine bereits bestehende Full Control-Sitzung in den View Only-Modus versetzt wird.

► Widerrufen Sie mit *Cancel*, wenn Sie nicht in den Full Control-Modus wechsel wollen.

Disconnect Session...

Eine fremde AVR-Sitzung beenden.

Mit *Disconnect Session* können Sie nur fremde AVR-Sitzungen beenden. Um Ihre eigene Sitzung zu beenden, wählen Sie *Exit*.

Es wird die Liste der aktuellen AVR-Sitzungen angezeigt:

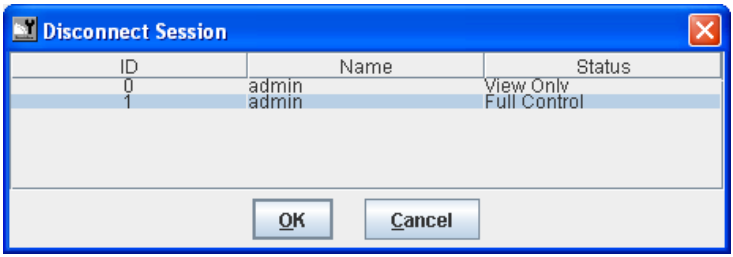


Bild 50: Menü Extras - Disconnect Session

- Markieren Sie die AVR-Sitzung, die Sie beenden wollen.
- Bestätigen Sie mit *OK*, wenn Sie die ausgewählte AVR-Sitzung beenden wollen.
- Widerrufen Sie mit *Cancel*, wenn Sie die ausgewählte AVR-Sitzung nicht beenden wollen.

Relinquish Full Control...

In den View Only-Modus wechseln. (Falls Sie sich bereits im View Only-Modus befinden, ist diese Funktion deaktiviert.)

Exit

Die eigene AVR-Sitzung beenden.

5.3.2 Menü Remote Storage

Unter *Remote Storage* rufen Sie die Remote Storage-Funktionalität auf:

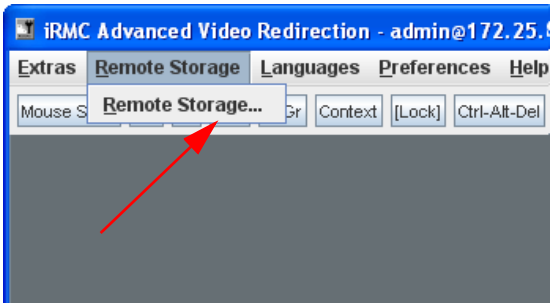


Bild 51: Fenster der Advanced Video Redirection - Menü Extras

Remote Storage...

Mit Doppelklick auf *Remote Storage...* öffnen Sie die Dialogbox *Storage Devices* (siehe Seite 162). In diesem Fenster können Sie Medien vom Remote-Arbeitsplatz als Remote Storage verbinden oder trennen (siehe Kapitel „Remote Storage“ auf Seite 159).

5.3.3 Menü Languages

Unter *Languages* wählen Sie die Landessprache aus, in der die Menüs und Dialoge des AVR-Fensters angezeigt werden:

Bild 52: Fenster Advanced Video Redirection - Menü Languages

5.3.4 Menü Preferences

Das Menü *Preferences* enthält Registerkarten für die Konfiguration von Maus, Tastatur und Logging sowie eine Registerkarte *Misc* für weitere Funktionen:

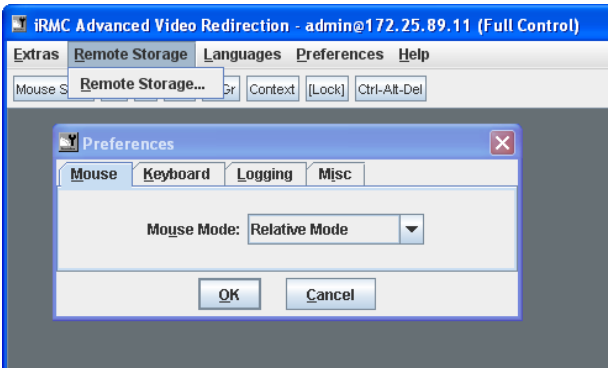


Bild 53: Fenster Advanced Video Redirection - Menü Preferences

Registerkarte Mouse

Mit der Registerkarte *Mouse* legen Sie den Mouse Mode fest:

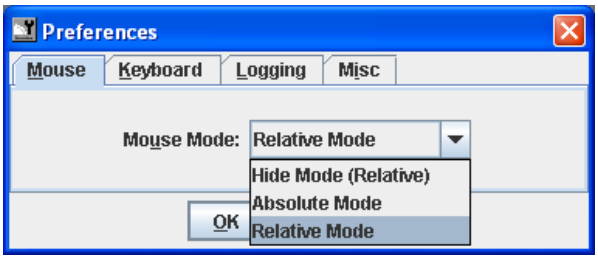


Bild 54: Menü Preferences - Registerkarte Mouse

Je nach Server-Betriebssystem müssen Sie folgende Einstellungen wählen:

– Windows: *Absolute Mode*, *Hide Mode (Relative)* oder *Relative Mode*
– Linux: *Hide Mode (Relative)*, *Relative Mode*

Default-Einstellung: *Relative Mode*

► Bestätigen Sie Ihre Eingaben mit *OK*.

Registerkarte Keyboard

Mit der Registerkarte *Keyboard* legen Sie das Tastatur-Layout für die virtuelle Konsole fest:

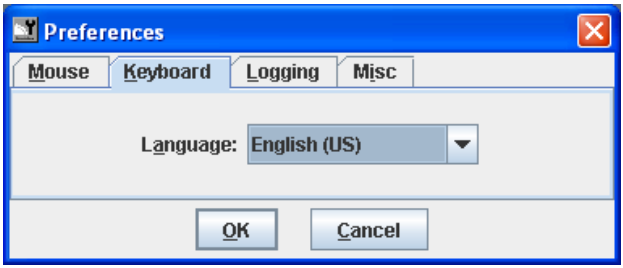


Bild 55: Menü Preferences - Registerkarte Keyboard

Language

Wählen Sie das Tastatur-Layout für die virtuelle Konsole aus.

Auch das Layout für die Tastatur am verwalteten Server muss entsprechend eingestellt sein.

- Bestätigen Sie Ihre Eingaben mit *OK*.

Registerkarte Logging

Mit der Registerkarte *Logging* konfigurieren Sie die Einstellungen für das Logging.

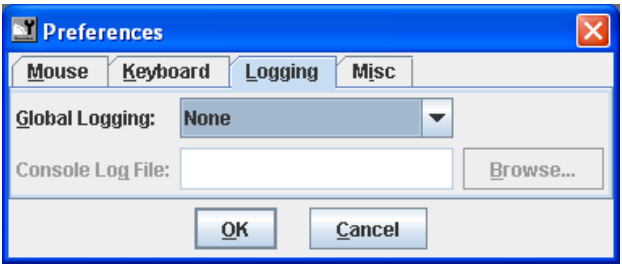


Bild 56: Menü Preferences - Registerkarte Logging

None muss eingestellt sein!

- Bestätigen Sie Ihre Eingaben mit *OK*.

Registerkarte Misc

Mit der Registerkarte *Misc* konfigurieren Sie, ob der iRMC Hardware-Komprimierung für die AVR-Sitzung durchführt.

Bild 57: Menü Preferences - Registerkarte Logging

Overwrite Native Storage Library
Diese Option ist für Sie nicht von Bedeutung.

Video Encryption
Wenn Sie diese Option aktivieren, führt der iRMC Verschlüsselung für die AVR-Sitzung durch.

► Bestätigen Sie Ihre Eingaben mit *OK*.

6 Remote Storage

Die Nutzung des Features „Remote Storage“ setzt einen gültigen License Key voraus.

Remote Storage stellt dem verwalteten Server ein „virtuelles“ Laufwerk zur Verfügung, das sich an anderer Stelle im Netz befindet. Es können bis zu zwei Medien umgeleitet werden.

Die Source für das virtuelle Laufwerk können Sie wie folgt bereitstellen:

– Mithilfe des AVR Java-Applets als physisches Laufwerk oder Image-File am Remote Arbeitsplatz (siehe Seite 160).

– Über einen Remote Storage Server zentral im Netz als Image-File (siehe Seite 169).

Parallele Remote Storage-Verbindungen:

Zur selben Zeit möglich sind entweder

– **maximal zwei** Remote Storage-Verbindungen zu virtuellen Laufwerken am Remote-Arbeitsplatz (bei Verbindungsaufbau via AVR Java-Applet)

oder

– **eine** Remote Storage-Verbindung zu einem Remote Storage Server.

Remote Storage-Verbindungen via Applet und Remote Storage Server sind nicht gleichzeitig möglich.

Mithilfe der Seite *Remote Storage* der iRMC-Web-Oberfläche können Sie sich über den Status der aktuellen Remote Storage-Verbindungen informieren und außerdem die Verbindung zu einem Remote Storage Server herstellen (siehe Seite 300).

6.1 Remote Storage am Remote-Arbeitsplatz bereitstellen

Wenn Sie die Source für ein virtuelles Laufwerk am Remote Arbeitsplatz bereitstellen, unterstützt Remote Storage folgende Gerätetypen:

- ISO Image (Image-File)
- Floppy-Disk
- USB Memory Device (z.B. Memory Stick)
- CD-ROM
- DVD-ROM

Mithilfe des virtuellen Laufwerks können Sie vom Remote-Arbeitsplatz aus auf Ihrem PRIMERGY Server ein Betriebssystem installieren (siehe Kapitel „IPMI OEM-Kommandos“ auf Seite 419).

Der vorliegende Abschnitt informiert über folgende Themen:

- Remote Storage starten.
- Speichermedien für Remote Storage bereitstellen.
- Speichermedien als Remote Storage verbinden.
- Remote Storage-Verbindungen trennen
- Für Remote Storage bereitgestellte Speichermedien entfernen.

6.1.1 Remote Storage starten

Remote Storage starten Sie über das AVR Java Applet (siehe Abschnitt „Advanced Video Redirection - Advanced Video Redirection (AVR) starten“ auf Seite 292):

- Starten Sie die iRMC-Web-Oberfläche (siehe Abschnitt „An der iRMC-Web-Oberfläche anmelden“ auf Seite 182).
- Öffnen Sie die Seite *Advanced Video Redirection* und klicken Sie auf die Schaltfläche *Start Video Redirection,* um die Advanced Video Redirection zu starten (siehe Abschnitt „Advanced Video Redirection - Advanced Video Redirection (AVR) starten“ auf Seite 292).

  Das AVR-Fenster wird geöffnet.
- Wählen Sie in der Menüleiste des AVR-Fensters:
  Remote Storage - RemoteStorage...

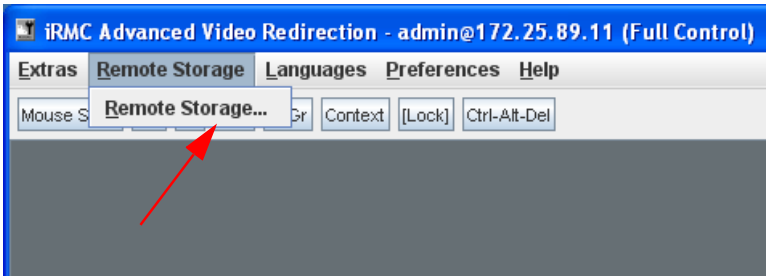


Bild 58: Fenster der Advanced Video Redirection - Remote Storage - Remote Storage...

Die Dialogbox *Storage Devices* wird geöffnet, in dem die aktuell für Remote Storage bereit gestellten Speichermedien angezeigt werden (siehe Bild 59 auf Seite 162).

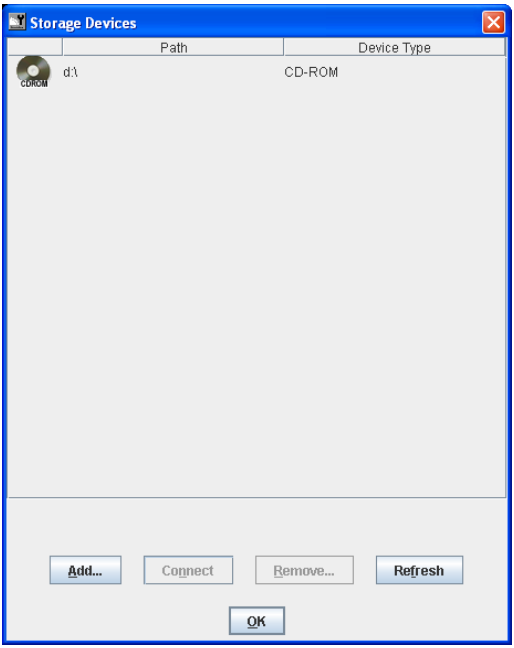


Bild 59: Dialogbox Storage Devices

Wenn in einem Laufwerk (CD-ROM, DVD-ROM) ein Speichermedium eingelegt ist, wird das Speichermedium automatisch angezeigt.

Falls ein Speichermedium eingelegt ist, aber nicht angezeigt wird, ist dieses Speichermedium durch den lokalen Explorer belegt.

6.1.2 Speichermedien für Remote Storage bereitstellen

► Klicken Sie in der Dialogbox *Storage Devices* auf die Schaltfläche *Add...* .

Die Dialogbox *Add Storage Device* wird geöffnet:

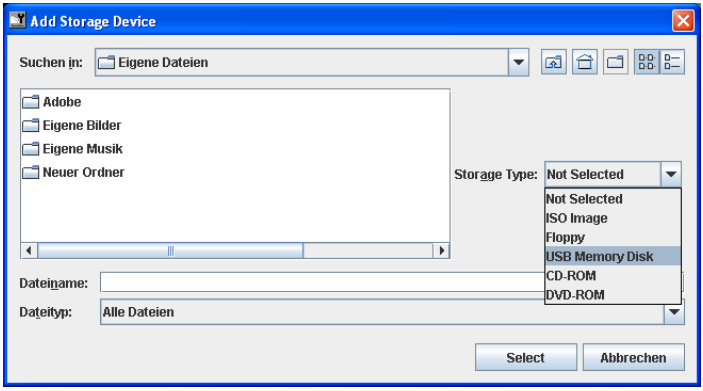


Bild 60: Dialogbox Add Storage Device

► Navigieren Sie in der Dialogbox *Add Storage Device* zum Verzeichnis des Speichermediums, das Sie von Ihrem Remote-Arbeitsplatz aus für Remote Storage bereitstellen wollen.

► Wählen Sie unter *Storage Type:* den gewünschten Gerätetyp aus.

Folgende Gerätetypen werden unterstützt:

- ISO Image (Image-File)
- Floppy-Disk
- USB MemoryDevice (z.B. USB Memory Stick)
- CD-ROM
- DVD-ROM

► Geben Sie unter *Dateiname:* das Speichermedium an, das Sie als Remote Storage verbinden wollen:

- Bei einem Image-File (ISO/NRG Image) geben Sie den Dateinamen an. Alternativ klicken auf den im Datei-Browser angezeigten Dateinamen.
- Bei einem Laufwerk geben Sie den Namen des Laufwerks an, z.B.
  - „D:“ für Laufwerk D (Windows)
  - */dev/...* (Linux)

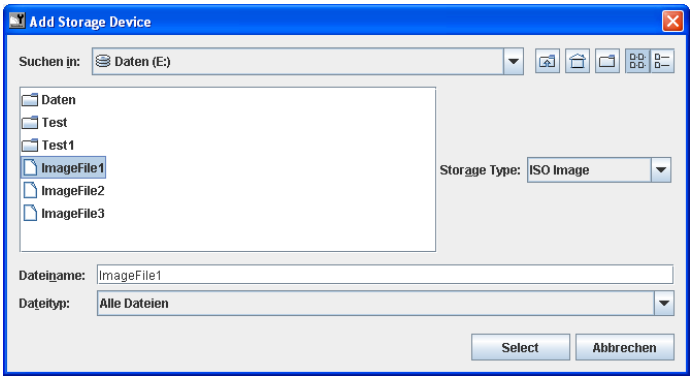


Bild 61: Dialogbox Add Storage Device: Speichermedium auswählen

► Klicken Sie auf *Select*, um Ihre Auswahl zu bestätigen.

Das ausgewählte Speichermedium ist für Remote Storage bereitgestellt und wird in der Dialogbox *Storage Devices* angezeigt.

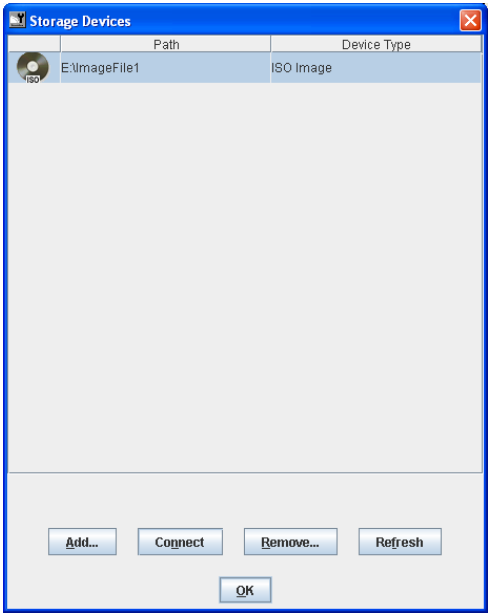


Bild 62: Dialogbox Storage Devices: Bereitgestelltes Speichermedium wird angezeigt.

6.1.3 Speichermedien als Remote Storage verbinden

► Markieren Sie in der Dialogbox *Storage Devices* das Speichermedium, das Sie als Remote Storage verbinden wollen.

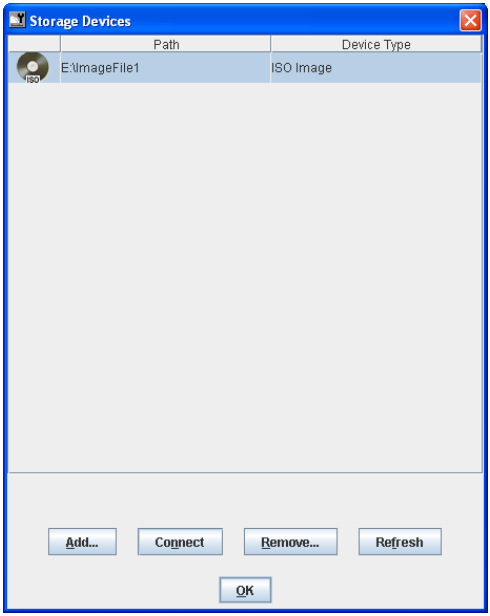


Bild 63: Dialogbox Storage Devices: Speichermedium als Remote Storage verbinden

► Klicken Sie auf *Connect*, um das ausgewählte Speichermedium als Remote Storage zu verbinden.

Es wird die Dialogbox *Storage Devices* mit dem Hinweis auf „Safe Remove“ angezeigt. Das Speichermedium ist als Remote Storage verbunden.

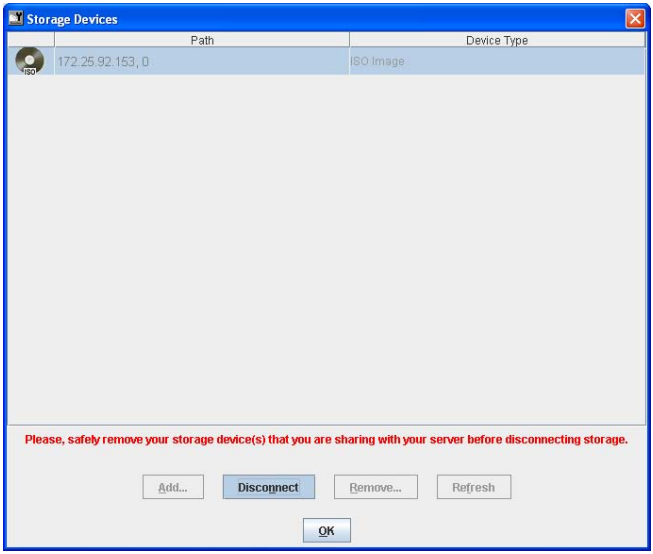


Bild 64: Dialogbox Storage Devices: Speichermedium ist als Remote Storage verbunden

6.1.4 Remote Storage-Verbindungen trennen

► Öffnen Sie die Dialogbox *Storage Devices* (siehe Abschnitt „Remote Storage starten“ auf Seite 161).

Die Liste der als Remote Storage verbundenen Speichermedien wird angezeigt:

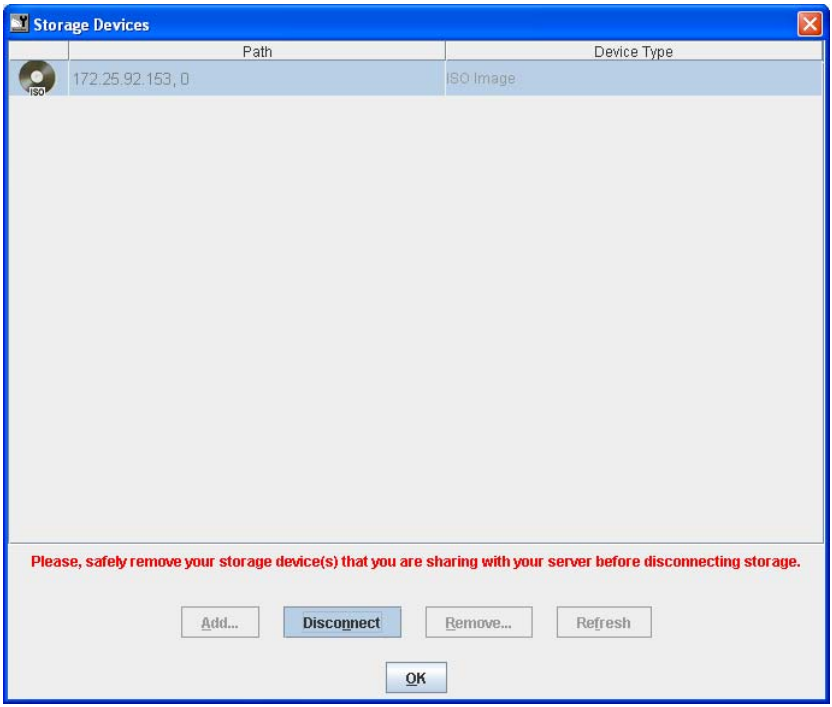


Bild 65: Dialogbox Storage Devices: Remote Storage-Verbindungen trennen

► Führen Sie einen „Safe Remove“ für die angezeigten Speichermedien durch, d.h. stellen Sie sicher, dass keine Anwendungen/Programme mehr auf die Speichermedien zugreifen.

► Klicken Sie auf *Disconnect...*, um alle Remote Storage-Verbindungen zu trennen.

6.1.5 Speichermedien entfernen

Aus der Liste der für Remote Storage bereitgestellten Speichermedien entfernen Sie ein Speichermedium wie folgt:

- ► Öffnen Sie die Dialogbox *Storage Devices* (siehe Abschnitt „Remote Storage starten“ auf Seite 161).

  Die Liste der für Remote Storage bereitgestellten Speichermedien wird angezeigt:

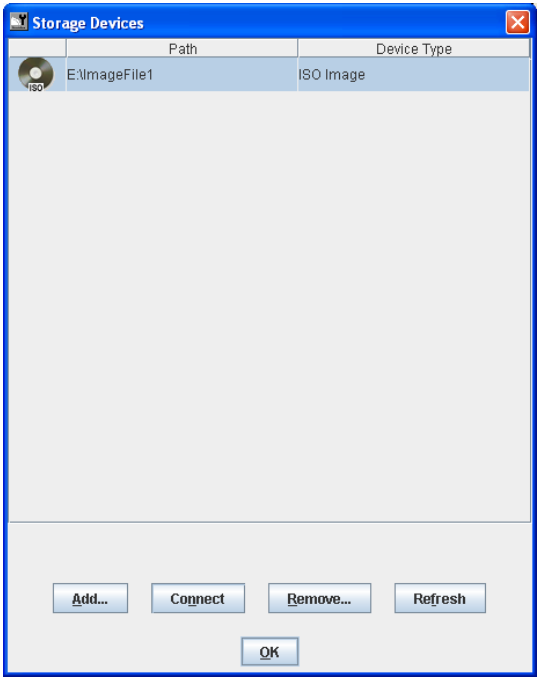


Bild 66: Dialogbox Storage Devices: Remote Storage Speichermedium entfernen

- ► Markieren Sie das Speichermedium, das Sie entfernen wollen.
- ► Klicken Sie auf *Remove...*, um das Speichermedium zu entfernen.

6.2 Remote Storage via Remote Storage Server bereitstellen

Mithilfe eines Remote Storage Servers können Sie für beliebige via iRMC administrierbare PRIMERGY Server in Ihrem Netz ein Image-File (ISO/NRG Image) als Remote Storage zur Verfügung stellen. Dieses Image-File können Sie verwenden, um vom Remote-Arbeitsplatz aus einen oder mehrere PRIMERGY Server zu booten (siehe Kapitel „IPMI OEM-Kommandos“ auf Seite 419).

Damit Ihr PRIMERGY Server das vom Remote Storage Server bereitgestellte Image-File nutzen kann, müssen folgende Voraussetzungen erfüllt sein:

- Der Remote Storage Server ist installiert (siehe Seite 170).
- Der Remote Storage Server ist gestartet (siehe Seite 179).
- Der iRMC des verwalteten Servers ist mit dem Remote Storage Server verbunden (siehe Seite 301).

6.2.1 Remote Storage Server installieren

Auf der ServerStart Software DVD finden Sie das Installationsprogramm *RemoteStorageServer_Installer32.exe* zur Installation des Remote Storage Servers.

Der Remote Storage Server ist in einer 32 bit- sowie einer 64 bit-Variante verfügbar. Auf 64 bit-Systemen darf nicht gleichzeitig die 32 bit- und 64 bit-Version des Remote Storage Servers installiert sein.

- Starten Sie *RemoteStorageServer_Installer32.exe*, um den Remote Storage Server zu installieren.

  Der Begrüßungsbildschirm des Installationsprogramms wird angezeigt:

Setup - Remote Storage Server
Welcome to the Remote Storage Server Setup Wizard
This will install RemoteStorageServer 2.0 on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
FUJITSU
Next >
Cancel

Bild 67: Remote Storage Server-Installation: Begrüßungsbildschirm

- Klicken auf die Schaltfläche *Next*.

  Das Fenster zur Festlegung des Installationsverzeichnisses wird angezeigt (siehe Bild 68 auf Seite 171).

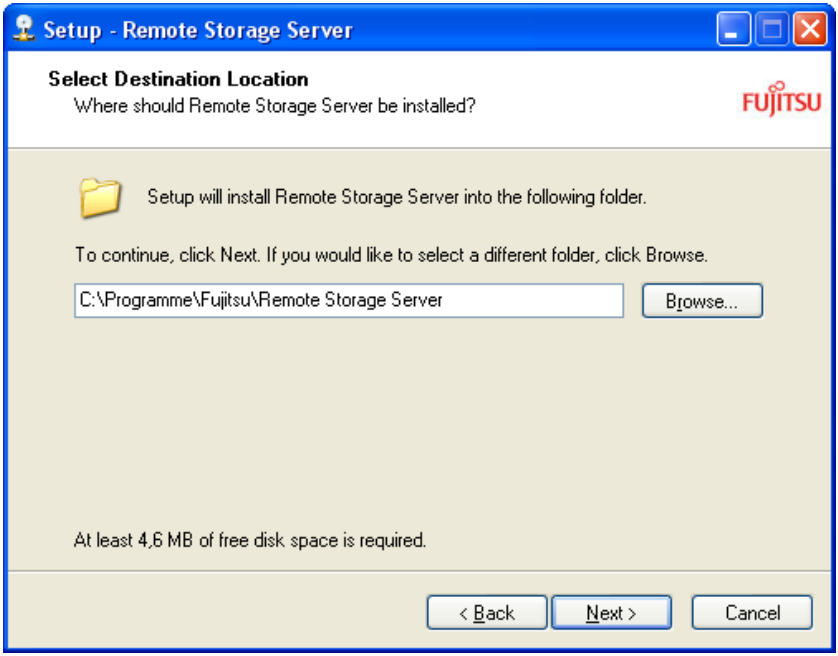

Setup - Remote Storage Server
Select Destination Location
Where should Remote Storage Server be installed?
FUJITSU
Setup will install Remote Storage Server into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Programme\Fujitsu\Remote Storage Server
Browse...
At least 4,6 MB of free disk space is required.
< Back
Next >
Cancel

Bild 68: Remote Storage Server-Installation: Installationsverzeichnis festlegen

- Falls Sie den Remote Storage Server nicht im voreingestellten Verzeichnis installieren wollen: Navigieren Sie über die Schaltfläche *Browse...* zum gewünschten Verzeichnis.
- Klicken auf die Schaltfläche *Next*.

  Das Fenster zur Platzierung der Programmverknüpfung im Startmenü wird angezeigt (siehe Bild 69 auf Seite 172).

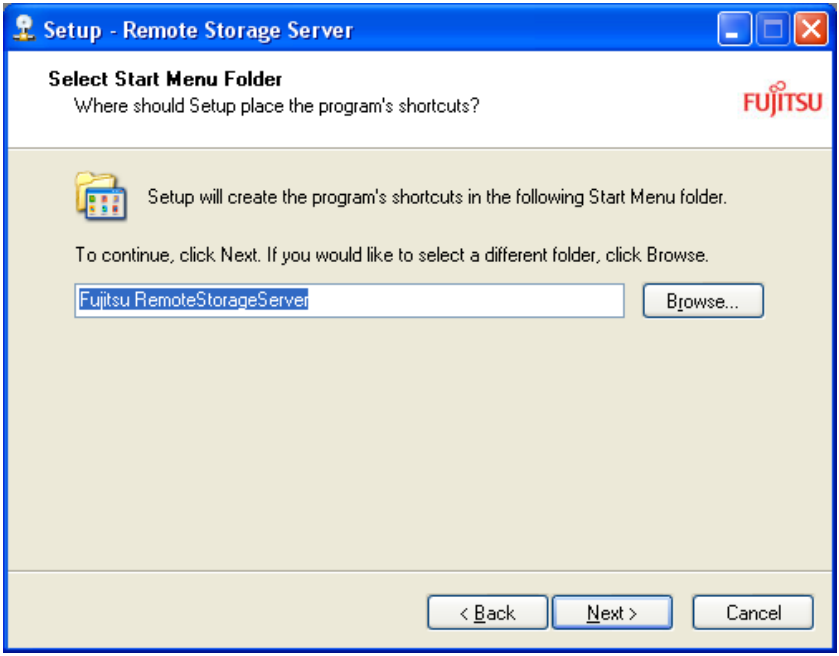

Setup - Remote Storage Server
Select Start Menu Folder
Where should Setup place the program's shortcuts?
FUJITSU
Setup will create the program's shortcuts in the following Start Menu folder.
To continue, click Next. If you would like to select a different folder, click Browse.
Fujitsu RemoteStorageServer
Browse...
< Back
Next >
Cancel

Bild 69: Remote Storage Server-Installation: Installationsverzeichnis festlegen

- Falls die Programmverknüpfung nicht im voreingestellten Ordner platziert werden soll: Legen Sie über die Schaltfläche *Browse...* den gewünschten Ordner fest.
- Klicken auf die Schaltfläche *Next*.

  Das Fenster *Ready to Install* wird geöffnet, in dem Sie die vorgenommenen Einstellungen kontrollieren und die Remote Storage Server-Installation starten können (siehe Bild 70 auf Seite 173).

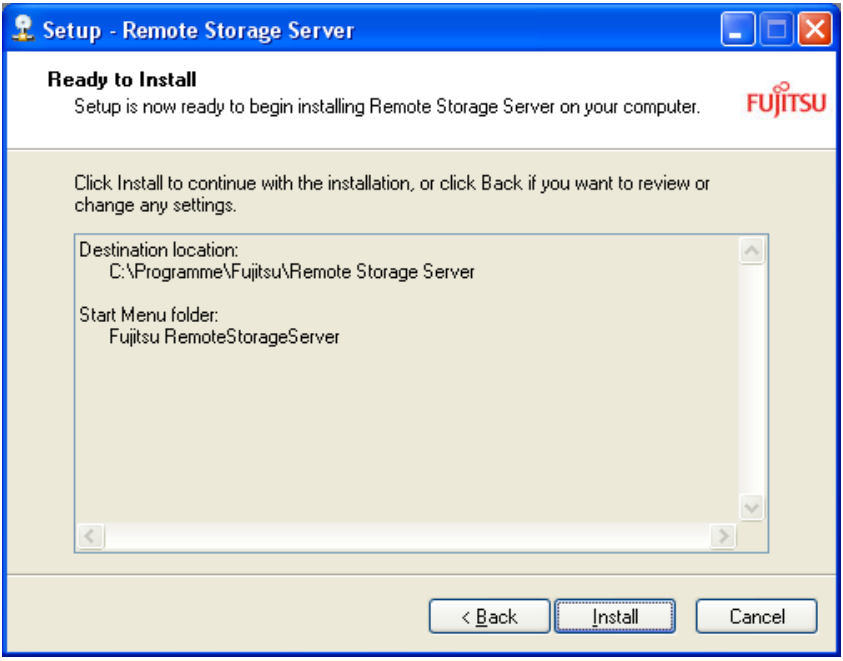

Setup - Remote Storage Server
Ready to Install
Setup is now ready to begin installing Remote Storage Server on your computer.
FUJITSU
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Programme\Fujitsu\Remote Storage Server
Start Menu folder:
Fujitsu RemoteStorageServer
< Back
Install
Cancel

Bild 70: Remote Storage Server-Installation: Installation starten

► Klicken auf die Schaltfläche *Install*, um die Remote Storage Server-Installation zu starten.

Nach Abschluss des Installationsvorgangs wird das Bild 71 auf Seite 174 dargestellte Fenster angezeigt.

Setup - Remote Storage Server
Completing the Remote Storage Server Setup Wizard
Setup has finished installing Remote Storage Server on your computer. The application may be launched by selecting the installed icons.
Click Finish to exit Setup.
Launch Remote Storage Server
FUJITSU
Finish

Bild 71: Remote Storage Server-Installation: Installationsprogramm beenden

Wenn Sie die Option *Launch Remote Storage Server* aktivieren, wird die grafische Bedienoberfläche des Remote Storage Servers (siehe Seite 176) nach Beenden des Installationsprogramms automatisch gestartet.

- Klicken Sie auf die Schaltfläche *Finish*, um das Installationsprogramm zu beenden.

Nach erfolgreicher Installation enthält Ihr Installationsverzeichnis u.a. die Datei RemoteStorageServer.exe.

6.2.2 Ausführungsmodi des Remote Storage Servers

Den Remote Storage Server können Sie wahlweise in folgenden Modi ausführen:

– als Service im Hintergrund

– als eigenständiges (stand-alone) Programm

Den Ausführungsmodus des Remote Storage Servers konfigurieren Sie über eine grafische Bedienoberfläche (siehe Seite 176).

Remote Storage Server als Service ausführen

Folgende Punkte sind zu beachten:

– Das Image-File kann wahlweise auf einem Rechner im Netz oder auf dem Rechner liegen, auf dem der Remote Storage Server läuft.

  Falls das Image-File nicht auf dem Rechner liegt, auf dem der Remote Storage Server läuft, müssen Sie den Pfad des Image-File in UNC-Notation angeben. Ferner benötigen Sie eine Benutzerkennung mit Zugriffsberechtigung auf das Image-File.

– Beim Booten des Rechners, auf dem der Remote Storage Server installiert ist, wird der Remote Storage Server automatisch gestartet. Der Remote Storage Server wird dann solange ausgeführt, bis er explizit beendet oder der Rechner heruntergefahren wird.

– Beim Booten des Rechners, auf dem der Remote Storage Server installiert ist, ist das Image-File automatisch verfügbar.

Remote Storage Server als eigenständiges Programm ausführen

Folgende Punkte sind zu beachten:

– Das Image-File (ISO/NRG Image) darf lokal auf dem Remote Storage Server oder auf einem zugeordneten Netzlaufwerk liegen.

– Beim Booten des Rechners, auf dem der Remote Storage Server installiert ist, müssen Sie das Image-File „von Hand“ starten.

6.2.3 Remote Storage Server konfigurieren, starten und beenden

Den Remote Storage Server konfigurieren, starten und beenden Sie über eine grafische Bedienoberfläche (GUI).

Grafische Bedienoberfläche des Remote Storage Servers aufrufen

Die grafische Bedienoberfläche des Remote Storage Servers rufen Sie wie folgt auf:

- Wählen Sie *Start - Alle Programme - Fujitsu RemoteStorageServer - Remote Storage Server*.

  Die grafische Bedienoberfläche des Remote Storage Servers wird angezeigt:

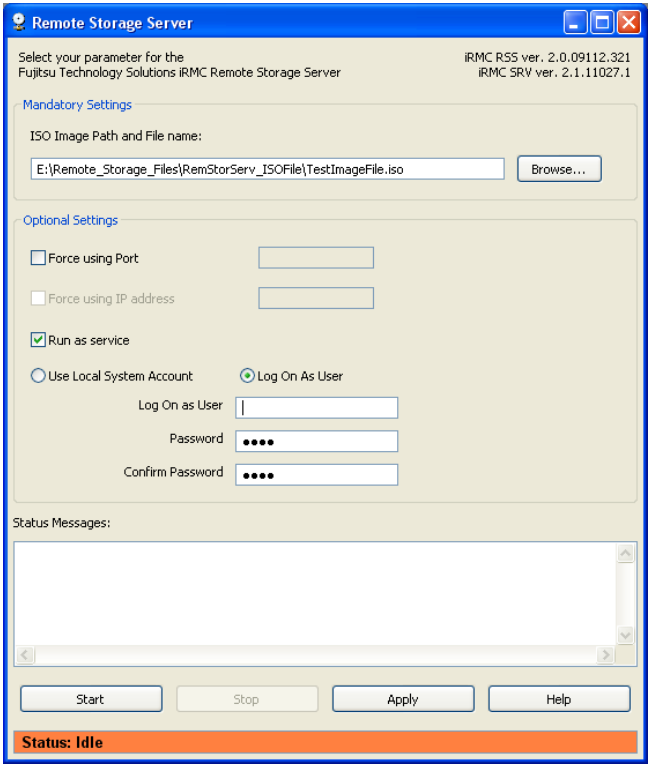


Bild 72: Grafische Bedienoberfläche des Remote Storage Servers (hier im Status „Idle“)

Remote Storage Server konfigurieren

Die Konfiguration setzt voraus, dass sich der Remote Storage Server im Status „idle“ befindet, also nicht ausgeführt wird.

Über die grafische Oberfläche spezifizieren Sie das als Remote Storage zur Verfügung gestellte Image-File sowie weitere Parameter:

ISO Image Path and Filename:

- Tragen Sie Pfad und Namen des Image-Files direkt im Eingabefeld ein.

  oder:

- Klicken Sie auf die Schaltfläche *Browse...* und selektieren Sie in der sich daraufhin öffnenden Dialogbox *Choose a file* das gewünschte Image-File per Navigieren und Bestätigungsdialog.

  Falls der Remote Storage Server als Service ausgeführt werden soll (siehe Option *Run as Service* auf Seite 178) und das Image-File auf einem Rechner im Netz liegt, müssen Sie den Pfad des Image-File in UNC-Notation spezifizieren. Stellen sie außerdem sicher, dass die unter *Log On As User* (siehe Seite 178) angegebene Benutzerkennung gültig ist und Zugriffsberechtigung für die freigegebene Netzwerk-Ressource besitzt, auf der das Image-File liegt.

Force Using Port

Wenn Sie für den Remote Storage Port des iRMC eine von der Default-Portnummer (5901) abweichende Portnummer konfiguriert haben (siehe Seite 246 oder Seite 349), müssen Sie diese Option aktivieren und im zugehörigen Eingabefeld die konfigurierte Portnummer eintragen.

Force Using IP Address

Falls der Rechner, auf dem der Remote Storage Server ausgeführt wird, über mehr als einen LAN-Anschluss verfügt:
Hier können Sie die IP-Adresse des LAN-Anschlusses angeben, der für den Remote Storage Server verwendet werden soll, wenn dieser als Service ausgeführt wird.
Standardmäßig verwendet der Remote Storage Server den ersten gefundenen LAN-Anschluss.

Run as Service

Aktivieren Sie diese Option, wenn der Remote Storage Server als Service im Hintergrund ausgeführt werden soll (siehe Seite 175).

► Wählen Sie eine der beiden folgenden Optionen:

Use Local System Account

Der Remote Storage Server wird als Service unter der lokalen Systemkennung ausgeführt.

Das Image-File (ISO/NRG Image) muss in diesem Fall auf einem lokalen Laufwerk liegen.

Log On As User

Der Remote Storage Server wird als Service unter der Benutzerkennung ausgeführt, die Sie in den nachfolgenden Eingabefeldern spezifizieren.

Spezifizieren Sie den Benutzernamen in der Form:

– Für lokale Benutzer: *.\Logon-Name*

– Für Domänen-Benutzer:

DOMAIN\LogOnName
oder
LogOnName@DOMAIN<mailto:LogOnName@DOMAIN>

Bei aktivierter Option *Log On As User* kann das Image-File (ISO/NRG Image) auf einem Netzlaufwerk liegen. In diesem Fall muss die angegebene Benutzerkennung Zugriffsrechte auf das Netzlaufwerk besitzen, auf dem das Image-File liegt. Außerdem müssen Sie den Pfad des Image-File in UNC-Notation spezifizieren (siehe Eingabefeld *ISO Image Path or Filename* auf Seite 177).

► Klicken Sie auf die Schaltfläche *Apply*, um Ihre Einstellungen zu aktivieren.

Remote Storage Server starten

► Klicken Sie auf die Schaltfläche *Start*, um den Remote Storage Server als Service oder als eigenständiges Programm zu starten:

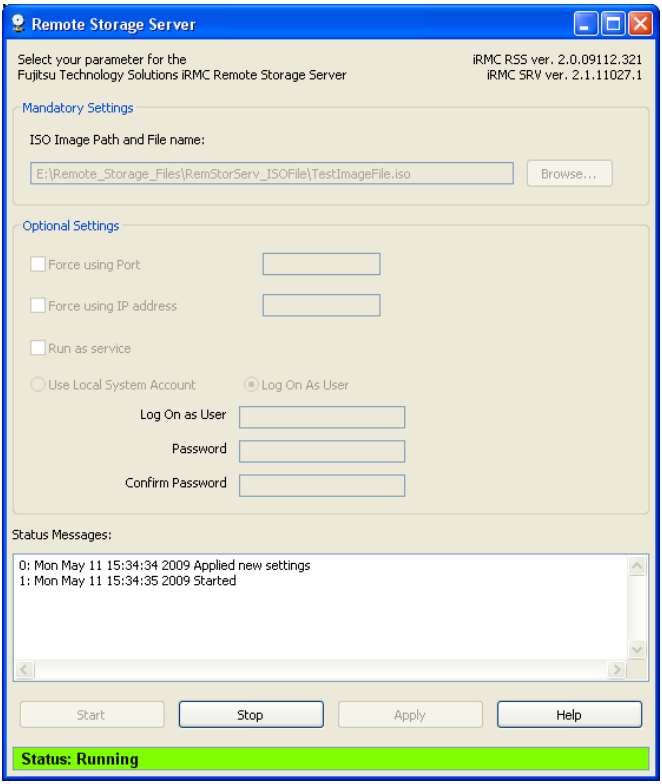


Bild 73: Remote Storage Server wird ausgeführt (Status „Running“)

Status Messages:

Hier werden die protokollierten Ausführungsstatus des Remote Storage Servers angezeigt.

Wenn der Ausführungsmodus *Run as service* konfiguriert ist (siehe Seite 178), wird der Remote Storage Server beim Booten des Rechners, auf dem der Remote Storage Server installiert ist, automatisch gestartet.

Die Ausführung des Remote Storage Servers wird bei Beenden der grafischen Bedienoberfläche nicht automatisch abgebrochen.

Remote Storage Server beenden

- Klicken Sie auf die Schaltfläche *Stop*, um die Ausführung des Remote Storage Servers zu beenden.

7 iRMC-Web-Oberfläche

Der iRMC verfügt nicht nur über ein eigenes Betriebssystem, sondern fungiert auch als Web-Server und bietet eine eigene Web-Oberfläche.

Sie können wählen, ob Sie sich die Menüs und Dialoge der iRMC-Web-Oberfläche in deutscher oder englischer Sprache anzeigen lassen möchten. Auch innerhalb derselben Sitzung können Sie zwischen den angebotenen Oberflächensprachen beliebig wechseln.

Bei der Eingabe von Werten an der iRMC-Web-Oberfläche erhalten Sie in vielen Fällen zusätzliche Unterstützung in Form von Tooltipps.

Die im Folgenden beschriebene Software basiert zum Teil auf den Arbeiten der Independent JPEG Group.

7.1 An der iRMC-Web-Oberfläche anmelden

► Öffnen Sie am Remote-Arbeitsplatz einen Web-Browser und geben Sie den (konfigurierten) DNS-Namen (siehe Seite 249) oder die IP-Adresse des iRMC ein.

Je nachdem, ob für den iRMC der LDAP-Zugriff auf einen Directory Service konfiguriert ist (Option *LDAP enabled*, siehe Seite 274), werden unterschiedliche Anmeldebildschirme angezeigt:

Falls kein Anmeldebildschirm angezeigt wird, überprüfen Sie die LAN-Verbindung (siehe Abschnitt „LAN-Schnittstelle testen“ auf Seite 43).

– LDAP-Zugriff des iRMC auf den Directory Service ist nicht konfiguriert (Option *LDAP enabled* ist nicht aktiviert):

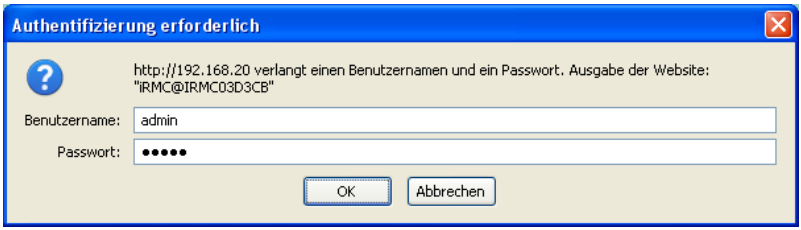


Bild 74: Anmeldebildschirm der iRMC-Web-Oberfläche (LDAP-Zugriff nicht konfiguriert)

► Geben Sie die Daten der Standard-Administratorkennung ein:

Benutzername: admin

Passwort: admin

Für *Benutzename* und *Passwort* wird zwischen Groß- und Kleinschreibung unterschieden.

Es wird empfohlen, wenn Sie sich angemeldet haben, aus Sicherheitsgründen eine neue Administratorkennung anzulegen und die Standard-Administratorkennung zu löschen oder zumindest das Passwort der Kennung zu ändern (siehe unter „User ’<name>’ Configuration - Benutzerkonfiguration (Details)“ auf Seite 266).

► Um zu bestätigen, klicken Sie auf die Schaltfläche *OK*.

– LDAP-Zugriff des iRMC auf den Directory Service ist konfiguriert (Option *LDAP enabled* oder Option *Always use SSL Login* ist aktiviert):

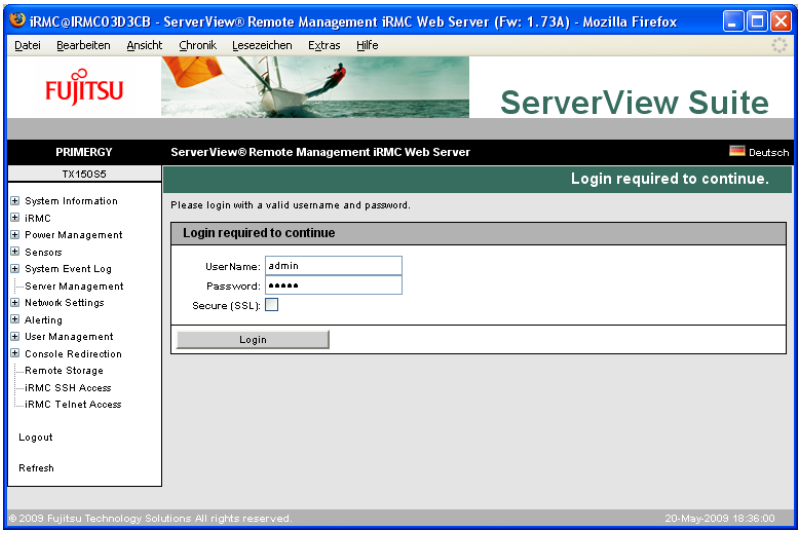


Bild 75: Anmeldebildschirm der iRMC-Web-Oberfläche (LDAP-Zugriff konfiguriert)

Benutzname und Passwort werden immer SSL-gesichert übertragen. Wenn Sie die Option *Secure (SSL)* aktivieren, erfolgt die gesamte Kommunikation zwischen Web-Browser und iRMC über HTTPS.

► Geben Sie die Daten der Standard-Administratorkennung ein:

Benutzername: admin

Passwort: admin

Es wird empfohlen, wenn Sie sich angemeldet haben, aus Sicherheitsgründen eine neue Administratorkennung anzulegen und die Standard-Administratorkennung zu löschen oder zumindest das Passwort der Kennung zu ändern (siehe unter „User '<name>' Configuration - Benutzerkonfiguration (Details)“ auf Seite 266).

► Um zu bestätigen, klicken Sie auf die Schaltfläche *Login*.

Die iRMC-Web-Oberfläche öffnet sich, die Seite *System Information* (siehe Seite 190) wird angezeigt.

7.2 Erforderliche Benutzerberechtigungen

Tabelle 4 gibt einen Überblick, welche Berechtigungen zur Nutzung der einzelnen an der iRMC-Web-Oberfläche angebotenen Funktionen erforderlich sind.

Funktion an iRMC-Web-Oberfläche	**Zulässig mit IPMI Privilege Level**				**Zulässig mit Berechtigung**			
	OEM	**Administrator**	**Operator**	**User**	**Configure User Accounts**	**Configure iRMC Settings**	**Video Redirection Enabled**	**Remote Storage Enabled**
Seiten *System Overview / Sytem Component Info.* öffnen.	X	X	X	X				
Identifizierungs-LED ein-/ausschalten.	X	X	X	X				
Seite *iRMC Information* öffnen.	X	X	X	X				
Firmware-Selektor setzen.	X	X						
License Key auf den iRMC laden.						X		
Seite *Save iRMC FW Settings* öffnen.					X	X		
Seite *Save iRMC FW Settings* (ohne *Incl. User Settings)*	X	X				X		
Seite *Save iRMC FW Settings* (*Include User Settings*)					X			
Seite *Certificate Upload* öffnen und bearbeiten.						X		
Seite *Generate a self signed RSA Cert.* öffnen u. bearb.						X		
Seite *Power On/Off* öffnen.	X	X	X	X				
Boot-Options ändern.						X		
Power Control anwenden.	X	X	X					
Seite *Power Options* öffnen und bearbeiten.						X		
Seite *Power Supply Info* öffnen.	X	X	X	X				
Seite *Fans* öffnen.	X	X	X	X				
Fan-Test starten (Gruppe *Fan Test*).	X	X	X	X				
Fan Check Time setzen (Gruppe *Fan Test*).						X		

Tabelle 4: Berechtigungen zur Nutzung der iRMC-Web-Oberfläche

Funktion an iRMC-Web-Oberfläche	**Zulässig mit IPMI Privilege Level**				**Zulässig mit Berechtigung**			
	OEM	**Administrator**	**Operator**	**User**	**Configure User Accounts**	**Configure iRMC Settings**	**Video Redirection Enabled**	**Remote Storage Enabled**
System Fans bearbeiten.						X		
Seite *Temperature* öffnen.	X	X	X	X				
Aktion bei kritischer Temperatur festlegen.						X		
Seite *Voltages* öffnen.	X	X	X	X				
Seite *Current* öffnen.	X	X	X	X				
Seite *Power Supply* öffnen.	X	X	X	X				
Seite *Component Status* öffnen.	X	X	X	X				
Seite *System Event Log Content* öffnen.	X	X	X	X				
System Event-Log (SEL) löschen.	X	X	X					
System Event-Log (SEL) sichern.	X	X	X	X				
Konfiguration des SEL ändern.						X		
Severity für Anzeige der SEL-Einträge festlegen.	X	X	X	X				
Seite *System Event Log Configuration* öffnen.	X	X	X	X				
Default Web Interface dispay filtering ändern.						X		
SEL-Modus (Ring / Puffer ändern.						X		
Seite *Server Management Info.* öffnen und bearbeiten.						X		
Seite *Network Interface* öffnen und bearbeiten.						X		
Seite *Ports and Netw. Services* öffnen und bearbeiten.						X		
Seite *DHCP Configuration* öffnen und bearbeiten.						X		
Seite *DNS Settings* öffnen und bearbeiten.						X		
Seite *SNMP TRAP Alerting* öffnen und bearbeiten.						X		
Seite *Serial / Modem Alerting* öffnen und bearbeiten.						X		
Seite *Email Alerting* öffnen und bearbeiten.						X		

Tabelle 4: Berechtigungen zur Nutzung der iRMC-Web-Oberfläche

Funktion an iRMC-Web-Oberfläche	Zulässig mit IPMI Privilege Level				Zulässig mit Berechtigung			
	OEM	Administrator	Operator	User	Configure User Accounts	Configure iRMC Settings	Video Redirection Enabled	Remote Storage Enabled
Seite *iRMC User* öffnen und bearbeiten.					X			
Seite *Directory Service Config.* öffnen und bearbeiten.						X		
Seite *BIOS Text Console* öffnen.	X	X	X	X				
BIOS Console Redirection Options verändern.						X		
Start Console Redirection durchführen.	X	X	X	X				
Logon im Fenster für Power-Mgmt. u. Text-Konsoluml.	X	X						
Text-Konsolumleitung starten (*Enter Console*).	X	X						
Seite *Adv. Video Redirection* öffnen und bearbeiten.							X	
Local Monitor ein/aus über Schaltfläche *Turn Off /On*	X	X					X	
Seite *Remote Storage* öffnen und bearbeiten.								X
iRMC SSH Access starten / *iRMC Telbnet Access* starten.	X	X	X	X				
SSH-Login / Telnet Login	X	X	X	X				

Tabelle 4: Berechtigungen zur Nutzung der iRMC-Web-Oberfläche

7.3 Aufbau der Bedienoberfläche

Die Bedienoberfläche der iRMC-Web-Schnittstelle ist wie folgt aufgebaut:

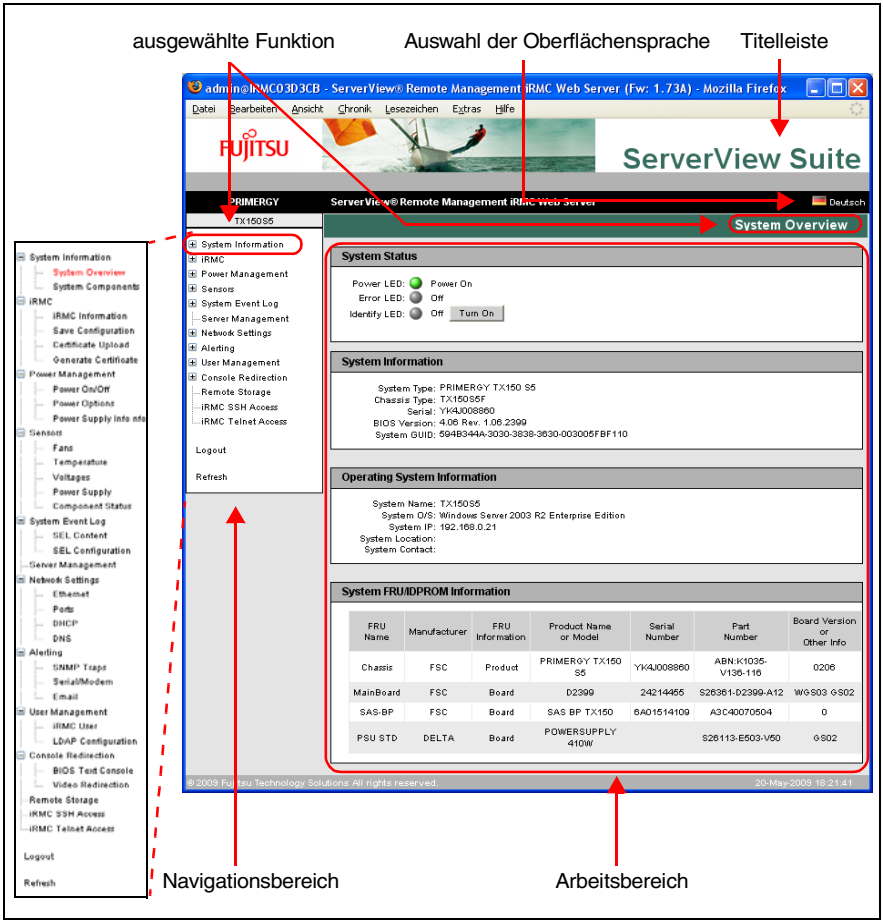


Bild 76: Aufbau der Bedienoberfläche der iRMC-Web-Oberfläche

Landessprache für die iRMC-Web-Oberfläche auswählen

In der schwarzen Leiste oberhalb des Arbeitsbereichs finden Sie rechts ein Flaggensymbol. Durch Klicken auf dieses Symbol wählen Sie die Landessprache (deutsch oder englisch) für die Anzeige von Navigationsbereich, Menüs und Dialogen der iRMC-Web-Oberfläche.

Navigationsbereich

Der Navigationsbereich enthält den Menübaum, dessen Knoten die Links zu den einzelnen iRMC-Funktionen aufgabenorientiert zusammenfassen. Wenn Sie einen dieser Links anklicken (in Bild 76: *System Overview*), wird der Link aktiviert und angezeigt wird der zur Funktion gehörige Arbeitsbereich mit Ausgaben, Dialogfeldern, Optionen, Links und Schaltflächen.

Unterhalb der Links zu den einzelnen iRMC-Funktionen finden Sie die Links *Logout* und *Refresh*:

- Mit *Logout* können Sie über einen Bestätigungsdialog die aktuelle iRMC-Session beenden. Je nachdem, ob für den iRMC der LDAP-Zugriff auf einen Directory Service konfiguriert ist (Option *LDAP enabled*, siehe Seite 274), werden nach Beendigung der Session unterschiedliche Login-Seiten angezeigt:
  - Falls der LDAP-Zugriff des iRMC auf den Directory Service nicht konfiguriert ist (Option *LDAP enabled* ist nicht aktiviert), wird die folgende Login-Seite angezeigt:

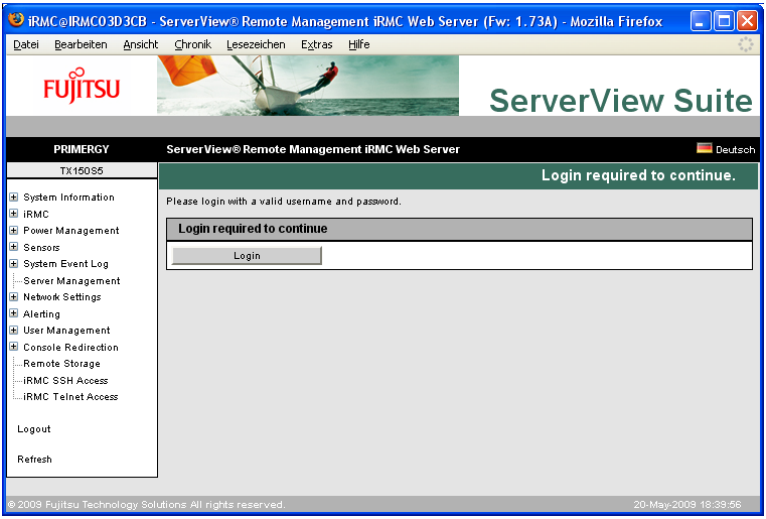


Bild 77: Login-Seite (nach Logout)

Durch Klicken auf die Schaltfläche *Login* gelangen Sie zum Anmeldebildschirm der iRMC-Web-Oberfläche, über den Sie sich erneut anmelden können (siehe Bild 74 auf Seite 182).

– Falls der LDAP-Zugriff des iRMC auf den Directory Service konfiguriert ist (Option *LDAP enabled* ist aktiviert), wird der entsprechende Anmeldebildschirm angezeigt (siehe Bild 75 auf Seite 183).

- Mit *Refresh* aktualisieren Sie die Anzeige der iRMC-Web-Oberfläche.

  Optional können Sie die automatische periodische Aktualisierung der Anzeige konfigurieren (siehe „Enable Auto Refresh“ auf Seite 244).

7.4 System Information - Informationen zum Server

Der Eintrag *System Information* enthält die Links auf folgende Seiten:

– „System Overview - Allgemeine Informationen zum Server“ auf Seite 191

– „System Component Information - Informationen zu den Server-Komponenten“ auf Seite 194

7.4.1 System Overview - Allgemeine Informationen zum Server

Die Seite *System Overview* liefert Informationen zu

- System-Status,
- System-Board,
- Betriebssystem des verwalteten Servers,
- System FRU (Field Replaceable Units) / IDPROM.

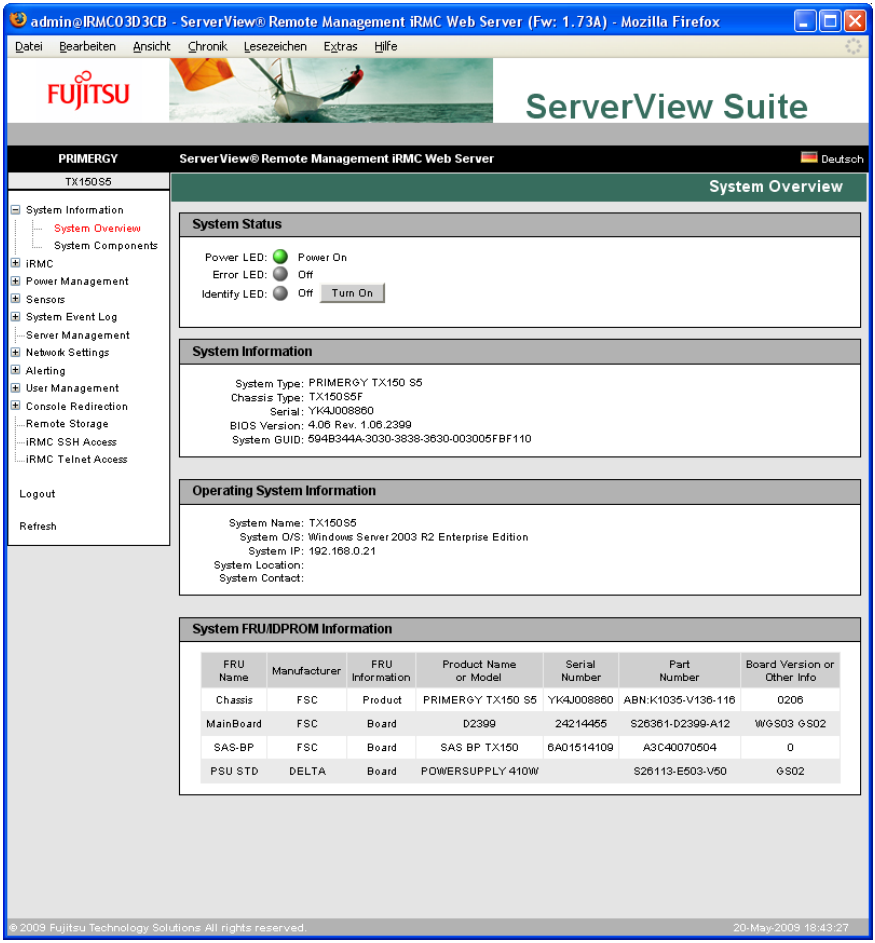


Bild 78: Seite System Overview

System Status

Unter *System Status* werden Sie über die Global Error-Anzeige am PRIMERGY Server informiert. Außerdem können Sie die PRIMERGY Identifizierungs-LED ein- und ausschalten.

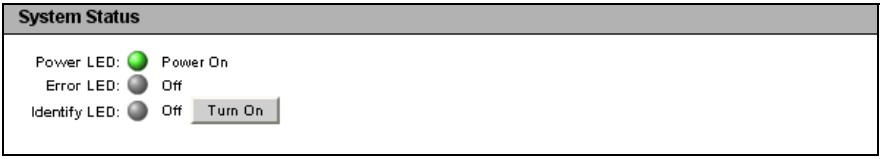


Bild 79: Seite System Overview - System Status

Power LED

Power-Zustand des Servers.
Folgende Status sind möglich:

- eingeschaltet: „Power ON“ (grün)
- ausgeschaltet: „Power OFF“ (orange))

Error LED

Informiert über Global Error-LED am Server:

Anzeige (iRMC)	Global Error LED am Server	Status des Servers
off	leuchtet nicht.	Es liegt kein kritisches Ereignis vor.
on	leuchtet rot.	Prefailure-Ereignis für eine Komponente.
blinking	blinkt rot.	Kritisches Ereignis.

Identify LED

Status der Identifizierungs-LED.
Folgende Status sind möglich:

- eingeschaltet: „ON“ (blau)
- ausgeschaltet: „ OFF“ (grau))

Turn On/ Turn Off

Durch Klicken auf die alternierende Schaltfläche *Turn On / Turn Off* können Sie die Identifizierungs-LED ein- bzw. ausschalten.

System FRU / IDPROM Information

Unter *Sytem FRU / IDPROM Information* sind Informationen zu den FRUs (**F**ield **R**eplaceable **U**nits) aufgelistet. FRUs sind Systemkomponenten, die freigegeben und aus dem System entfernt werden können.

7.4.2 System Component Information - Informationen zu den Server-Komponenten

Die Seite *System Component Information* liefert Informationen zu den CPUs.

Die möglichen Status der Systemkomponenten werden durch folgende Status-Icons symbolisiert:

	OK: Der Zustand der Komponente ist in Ordnung.
	Der Steckplatz für die Komponente ist leer.
	Warnung: Der Zustand der Komponente hat sich verschlechtert.
	Fehler: Die Komponente hat einen Fehler.

Tabelle 5: Status der Systemkomponente

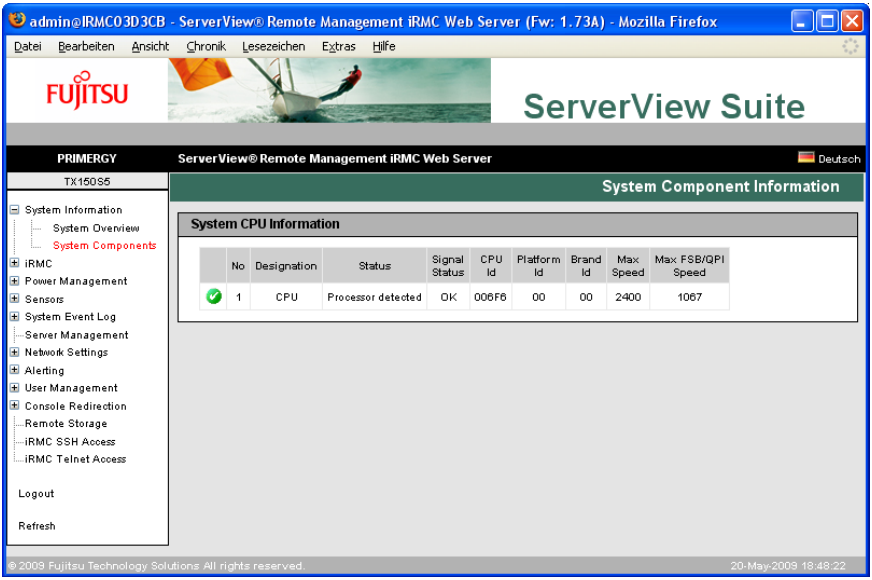


Bild 80: Seite System Component Information

7.5 iRMC - Informationen, Firmware und Zertifikate

Der *iRMC* enthält die Links auf folgende Seiten:

– „iRMC Information - Informationen zum iRMC“ auf Seite 196

– „Save iRMC Firmware Settings - Firmware-Einstellungen sichern“ auf Seite 200

– „Certificate Upload - DSA/RSA-Zertifikat und privaten DSA/RSA-Schlüssel laden“ auf Seite 202

– „Generate a self-signed RSA Certificate - Selbstsigniertes RSA-Zertifikat erzeugen“ auf Seite 208

7.5.1 iRMC Information - Informationen zum iRMC

Die Seite *iRMC Information* bietet Ihnen folgende Möglichkeiten:

– Informationen zu Firmware- und SDRR-Version des iRMC einsehen, den Firmware-Selektor setzen und den iRMC neu starten.

– Informationen zu den aktiven iRMC-Sessions einsehen.

– License Key auf den iRMC laden.

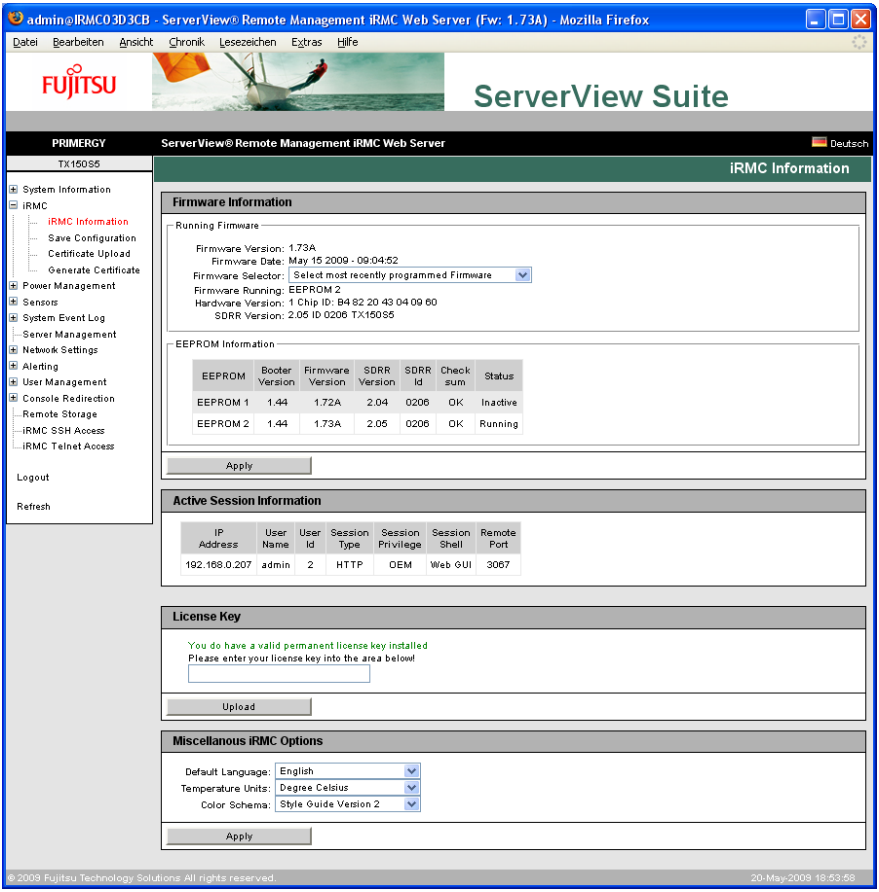

admin@IRMC03D3CB - ServerView® Remote Management iRMC Web Server (Fw: 1.73A) - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
FUJITSU
ServerView Suite
PRIMERGY
ServerView® Remote Management iRMC Web Server
Deutsch
TX150S5
iRMC Information
System Information
iRMC
iRMC Information
Save Configuration
Certificate Upload
Generate Certificate
Power Management
Sensors
System Event Log
Server Management
Network Settings
Alerting
User Management
Console Redirection
Remote Storage
iRMC SSH Access
iRMC Telnet Access
Logout
Refresh
Firmware Information
Running Firmware
Firmware Version: 1.73A
Firmware Date: May 15 2009 - 09:04:52
Firmware Selector: Select most recently programmed Firmware
Firmware Running: EEPROM 2
Hardware Version: 1 Chip ID: B4 82 20 43 04 09 60
SDRR Version: 2.05 ID 0206 TX150S5
EEPROM Information
EEPROM | Booter Version | Firmware Version | SDRR Version | SDRR Id | Check sum | Status
EEPROM 1 | 1.44 | 1.72A | 2.04 | 0206 | OK | Inactive
EEPROM 2 | 1.44 | 1.73A | 2.05 | 0206 | OK | Running
Apply
Active Session Information
IP Address | User Name | User Id | Session Type | Session Privilege | Session Shell | Remote Port
192.168.0.207 | admin | 2 | HTTP | OEM | Web GUI | 3067
License Key
You do have a valid permanent license key installed
Please enter your license key into the area below!
Upload
Miscellanous iRMC Options
Default Language: English
Temperature Units: Degree Celsius
Color Schema: Style Guide Version 2
Apply
© 2009 Fujitsu Technology Solutions All rights reserved.
20-May-2009 18:53:58

Bild 81: Seite iRMC Information

Firmware Information

Unter *Firmware Information* können Sie Informationen zu Firmware- und SDRR-Version des iRMC einsehen sowie den Firmware-Selektor setzen.

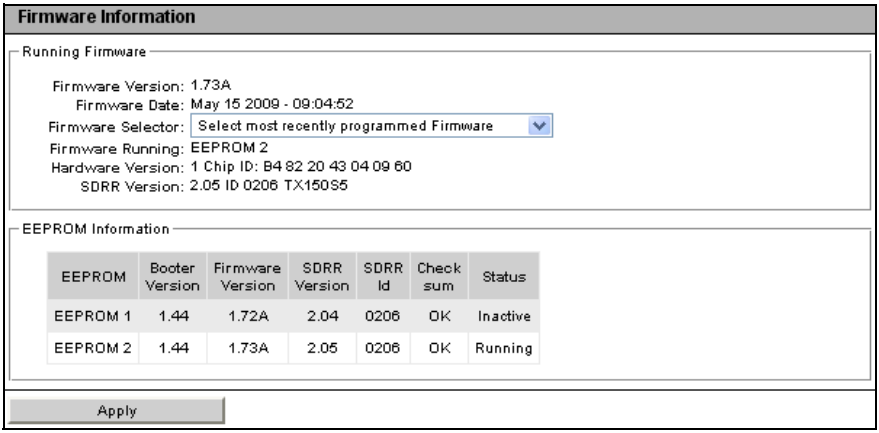

Firmware Information
Running Firmware
Firmware Version: 1.73A
Firmware Date: May 15 2009 - 09:04:52
Firmware Selector: Select most recently programmed Firmware
Firmware Running: EEPROM 2
Hardware Version: 1 Chip ID: B4 82 20 43 04 09 60
SDRR Version: 2.05 ID 0206 TX150S5
EEPROM Information
EEPROM | Booter Version | Firmware Version | SDRR Version | SDRR Id | Check sum | Status
EEPROM 1 | 1.44 | 1.72A | 2.04 | 0206 | OK | Inactive
EEPROM 2 | 1.44 | 1.73A | 2.05 | 0206 | OK | Running
Apply

Bild 82: Seite iRMC Information - Firmware Information

Firmware Selector

Mithilfe des Firmware-Selektors legen Sie fest, welches Firmware-Image nach dem nächsten Reboot des iRMC aktiv ist.

Folgende Möglichkeiten stehen zur Auswahl:

– *Auto - EEPROM with highest FW version*

  Es wird automatisch der EEPROM mit dem aktuellsten Versionsstand ausgewählt.

– *EEPROM1*

  Es wird EEPROM 1 ausgewählt.

– *EEPROM2*

  Es wird EEPROM 2 ausgewählt.

– *Select EEPROM with oldest FW version*

  Es wird das Firmware-Image mit dem ältesten Versionsstand ausgewählt.

– *Select most recently programmed FW*

  Es wird das zuletzt aktualisierte Firmware-Image ausgewählt.

– *Select least recently programmed FW*

  Es wird das am längsten nicht mehr aktualisierte Firmware-Image ausgewählt.

Apply

Mit *Apply* setzen Sie den Firmware-Selektor auf die unter *Firmware Selector* gewählte Einstellung.

License Key

Mit der Gruppe *License Key* können Sie einen License Key auf den iRMC laden.

Einen gültigen License Key benötigen Sie, um die iRMC-Funktionen *Advanced Video Redirection* (siehe Seite 292) und *Remote Storage* (siehe Seite 300) nutzen zu können.

Den License Key können Sie käuflich erwerben.

Upload

Wenn Sie auf diese Schaltfläche klicken, wird der im Eingabefeld spezifizierte License Key auf den iRMC geladen.

Miscellaneous iRMC Options

Mit der Gruppe *Miscellaneous iRMC Options* können Sie Einstellungen für das Layout der iRMC-Web-Oberfläche festlegen.

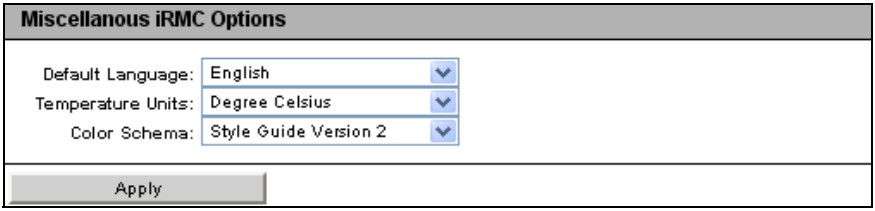


Bild 83: Seite iRMC Information - Miscellaneous iRMC Options

Default Language

Legt die Landessprache (Deutsch / Englisch) fest, die beim nächsten Aufruf der iRMC-Web-Oberfläche voreingestellt ist.

Temperature Units

Legt die Einheit für die Anzeige von Temperaturwerten an der iRMC-Web-Oberfläche fest (Grad Celsius / Grad Fahrenheit). Diese Einstellung gilt die aktuelle Sitzung und ist beim nächsten Aufruf der iRMC-Web-Oberfläche voreingestellt.

Colour Schema

Legt das Farbschema für die Anzeige der iRMC-Web-Oberfläche fest. Diese Einstellung gilt die aktuelle Sitzung und ist beim nächsten Aufruf der iRMC-Web-Oberfläche voreingestellt.

7.5.2 Save iRMC Firmware Settings - Firmware-Einstellungen sichern

Mithilfe der Seite *Save iRMC Firmware Settings* können Sie die aktuellen Firmware-Einstellungen sowie eine Reihe weiterer Einstellungen des iRMC in einer Datei abspeichern.

– Die unter *Save iRMC Firmware settings in ServerView® WinSCU XML format* ausgewählten Firmware-Settings werden in der Datei *iRMC_settings.pre* gesichert. Im WinSCU (siehe Seite 335) können Sie über die Schaltfläche *Import...* die Firmware-Settings wieder auf den iRMC laden.

– Die unter *Save iRMC Firmware settings in binary (BMCCLONE.exe) format* ausgewählten Firmware-Settings werden in der Datei *iRMC_settings.bin* gesichert.

ACHTUNG!

Sichern Sie die Einstellung grundsätzlich mithilfe von *Save iRMC Firmware settings in ServerView® WinSCU XML format*.

Save iRMC Firmware settings in binary (BMCCLONE.exe) format sollte nur bei Austausch der Systembaugruppe des verwalteten Servers verwendet werden.

Zum Sichern von Benutzereinstellungen *(Include User Settings*) ist *Configure User Accounts*-Berechtigung erforderlich, in den anderen Fällen genügt die *Configure iRMC settings*-Berechtigung.

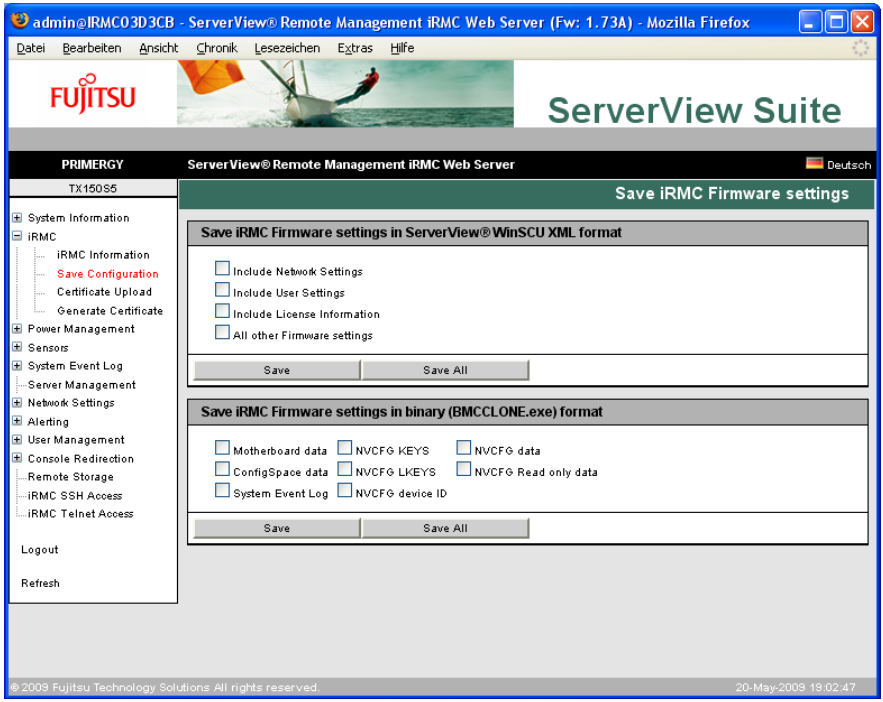


Bild 84: Seite Save iRMC Firmware Settings

Save

Mit *Save* sichern Sie die gewählten Einstellungen.

Save All

Mit *Save All* sichern Sie alle Einstellungen.

7.5.3 Certificate Upload - DSA/RSA-Zertifikat und privaten DSA/RSA-Schlüssel laden

Mit der Seite *Certificate Upload* können Sie ein von einer Certificate Authority (CA) signiertes X.509 DSA/RSA-Zertifikat (SSL) und/oder Ihren privaten DSA/RSA-Schlüssel (SSH) auf den iRMC laden.

Der iRMC wird mit einem vordefinierten Server-Zertifikat (Default-Zertifikat) ausgeliefert. Wenn Sie auf den iRMC über SSL/SSH-gesicherte Verbindungen zugreifen möchten, wird empfohlen, das Default-Zertifikat möglichst bald durch ein Zertifikat zu ersetzen, das von einer Certificate Authority (CA) signiert ist.

Eingabeformat von X.509 DSA/RSA-Zertifikat und privatem DSA/RSA-Schlüssel:

X.509 DSA/RSA-Zertifikat und privater RSA/DSA-Schlüssel müssen jeweils in PEM-Codierung (ASCII/Base64) vorliegen.

Bild 85: Seite Certificate Upload

Aktuell gültiges DSA/RSA-Zertifikat anzeigen

► Klicken Sie in der Gruppe *Certificate Information and Restore* auf die Schaltfläche *View Certificate*, um sich das aktuell gültige Zertifikat anzeigen zu lassen.

Bild 86: Seite Certificate Upload - Anzeige des aktuell gültigen SSL-/SSH-Zertifikats

Default-Zertifikat wiedereinsetzen

► Klicken Sie in der Gruppe *Certificate Information and Restore* auf die Schaltfläche *Default Certificate*, um nach einem Bestätigungsdialog das Default-Zertifikat wiedereinzusetzen, das mit der Firmware ausgeliefert wurde.

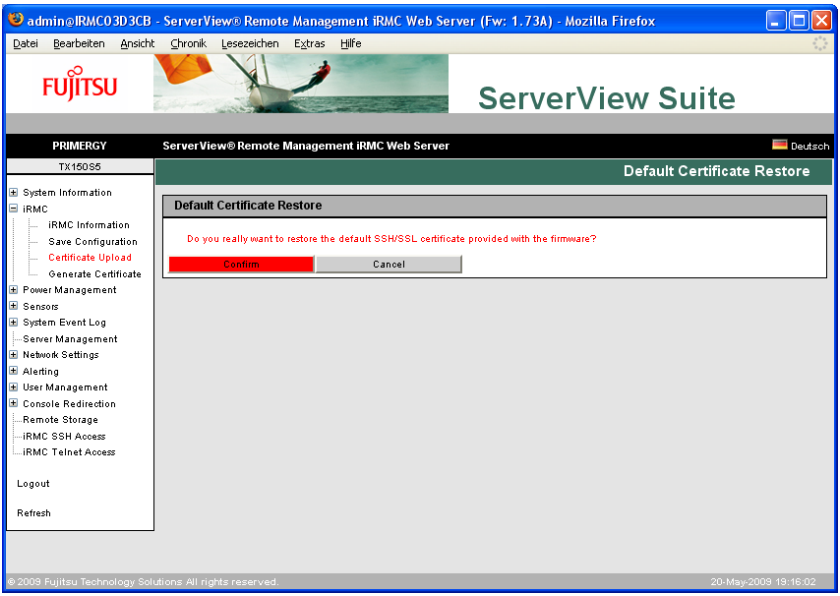


Bild 87: Seite Certificate Upload - Default-Zertifikat wiedereinsetzen

DSA/RSA-Zertifikat und privaten DSA/RSA-Schlüssel aus lokalen Dateien laden

Hierfür verwenden Sie die Gruppe
SSL Certificate and DSA/RSA private key upload from file

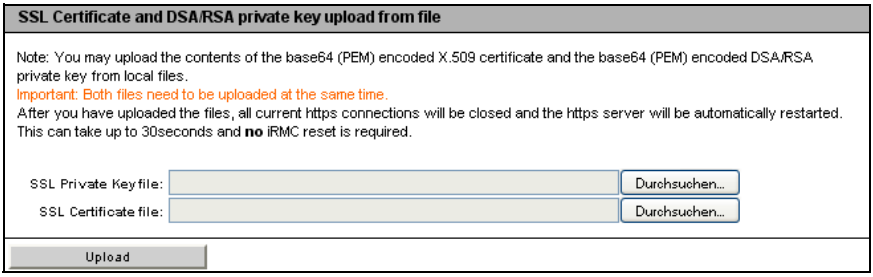


Bild 88: DSA/RSA-Zertifikat und privaten DSA/RSA-Schlüssel aus lokalen Dateien laden

Gehen Sie wie folgt vor:

- Speichern Sie das X.509 DSA/RSA (SSL)-Zertifikat und den privaten DSA/RSA-Schlüssel in entsprechenden lokalen Dateien des verwalteten Servers.
- Spezifizieren Sie die Dateien *Private Key File* und *Certificate File*, indem Sie jeweils auf die zughörige Schaltfläche *Durchsuchen* klicken und zur Datei navigieren, die den privaten Schlüssel bzw. das Zertifikat enthält.
- Kicken Sie auf die Schaltfläche *Upload,* um das Zertifikat und den privaten Schlüssel auf den iRMC zu laden.

  Beim Hochladen von Zertifikat und privatem Schlüssel werden alle bestehenden HTTPS-Verbindungen geschlossen, und der HTTPS Server wird automatisch neu gestartet. Dieser Vorgang kann bis zu 30 Sekunden dauern. Ein expliziter Reset des iRMC ist **nicht** erforderlich.
- Klicken Sie auf die Schaltfläche *View Certificate*, um sich vom erfolgreichen Laden des Zertifikats zu überzeugen.

DSA/RSA-Zertifikat / privaten DSA/RSA-Schlüssel direkt eingeben

Hierfür verwenden Sie die Gruppe
SSL DSA/RSA certificate or DSA/RSA private upload via copy & paste.

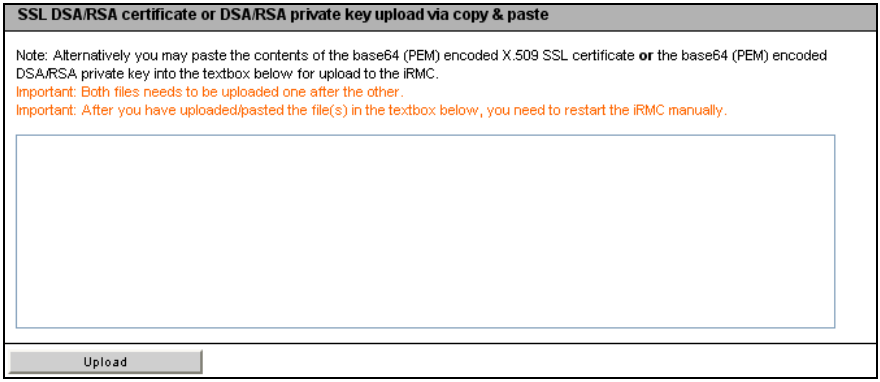


Bild 89: DSA/RSA-Zertifikat / privaten DSA/RSA-Schlüssel direkt eingeben

Gehen Sie wie folgt vor:

- Kopieren Sie das X.509 DSA-Zertifikat **oder** den privaten DSA-Schlüssel in den Eingabereich.

  Die gleichzeitige Eingabe von Zertifikat und Schlüssel für denselben Upload ist nicht zulässig.

- Kicken Sie auf die Schaltfläche *Upload,* um das Zertifikat oder den privaten Schlüssel auf den iRMC zu laden.

- Führen Sie mithilfe des Remote Manager einen Reset des iRMC durch (siehe Abschnitt „Service Processor - IP-Parameter, Identifizierungs-LED und Reset des iRMC“ auf Seite 325).

  Dies ist erforderlich, damit ein auf den iRMC geladenes Zertifikat oder privater Schlüssel gültig wird.

- Klicken Sie auf die Schaltfläche *View Certificate*, um sich vom erfolgreichen Laden des Zertifikats zu überzeugen.

7.5.4 Generate a self-signed RSA Certificate - Selbstsigniertes RSA-Zertifikat erzeugen

Mit der Seite *Generate a self-signed RSA Certificate* können Sie ein selbstsigniertes Zertifikat erstellen.

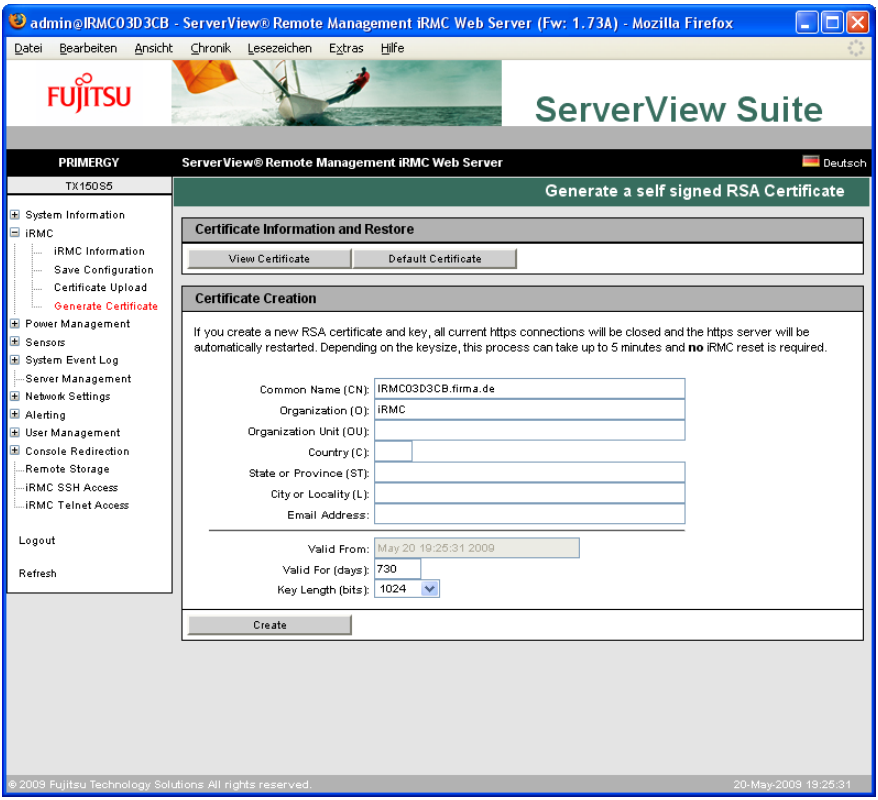


Bild 90: Seite Generate a self signed Certificate

View Certificate

Mithilfe dieser Schaltfläche können Sie sich das aktuell gültige DSA/RSA-Zertifikat anzeigen lassen.

Default Certificate

Mithilfe dieser Schaltfläche können Sie über einen Bestätigungsdialog das Default-Zertifikat wiedereinzusetzen, das mit der Firmware ausgeliefert wurde.

- Tragen Sie unter *Certificate Creation* die erforderlichen Angaben ein.
- Klicken Sie auf die Schaltfläche *Create*, um das Zertifikat zu erzeugen.

Beim Generieren des neuen Zertifikats werden alle bestehenden HTTPS-Verbindungen geschlossen, und der HTTPS Server wird automatisch neu gestartet. Je nach Schlüssellänge kann bis zu 5 Minuten dauern. Ein expliziter Reset des iRMC ist **nicht** erforderlich.

7.6 Power Management

Der Eintrag *Power Management* enthält die Links auf die Seiten für das Power Management Ihres PRIMERGY Servers:

– „Power On/Off - Server ein-/ausschalten“ auf Seite 211.

– „Power Options - Power Management des Servers konfigurieren“ auf Seite 215.

– „Power Supply Info - Stromversorgung und IDPROM-Daten der FRU-Komponenten“ auf Seite 218.

7.6.1 Power On/Off - Server ein-/ausschalten

Über die Seite *Power On/Off* können Sie den verwalteten Server ein- und ausschalten. Sie werden über den aktuellen Power-Status des Servers informiert und können außerdem das Verhalten des Servers beim nächsten Boot-Vorgang konfigurieren.

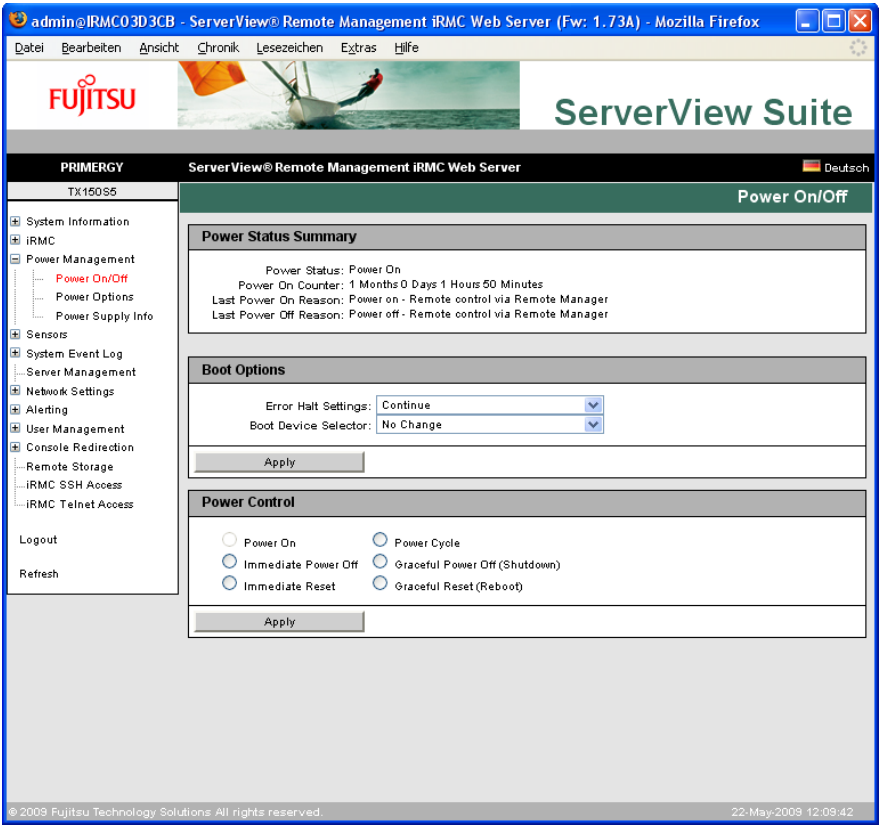


Bild 91: Seite Power On/Off

Power Status Summary

In der Gruppe *Power Status Summary* werden Sie über den aktuellen Power Status des Servers sowie über die Ursachen für das letzte An- und Abschalten informiert. Außerdem summiert ein Zähler die Jahre, Monate, Tage und Minuten, die der Server bisher insgesamt eingeschaltet war.

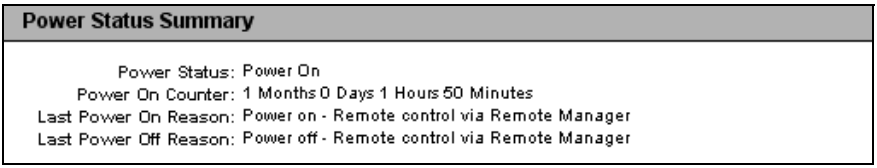

Power Status Summary
Power Status: Power On
Power On Counter: 1 Months 0 Days 1 Hours 50 Minutes
Last Power On Reason: Power on - Remote control via Remote Manager
Last Power Off Reason: Power off - Remote control via Remote Manager

Bild 92: Seite Power On/Off - Power Status Summary

Boot Options

Mit der Gruppe *Boot Options* konfigurieren Sie das Verhalten des Systems beim **nächsten** Bootvorgang. So können Sie einstellen, ob das BIOS den Bootvorgang des Systems unterbrechen soll, wenn während der POST-Phase Fehler auftreten.

Die hier eingestellten Optionen gelten nur für den nächsten Bootvorgang. Danach ist wieder der voreingestellte Mechanismus wirksam.

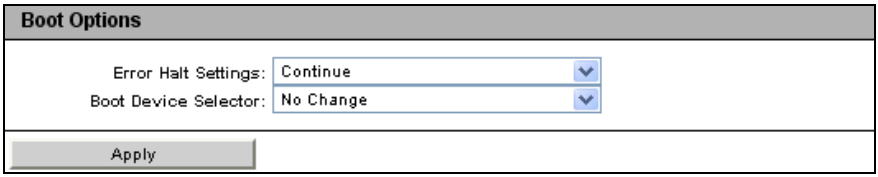


Bild 93: Seite Power On/Off - Boot Options

- Wählen Sie in der Liste *Error Halt Settings* das gewünschte BIOS-Verhalten:

  Continue
  Bootvorgang des Systems fortsetzen, wenn während der POST-Phase Fehler auftreten.

  Halt on errors
  Bootvorgang des Systems unterbrechen, wenn während der POST-Phase Fehler auftreten.

- Wählen Sie in der Liste *Boot Device Selector* das Speichermedium, von dem gebootet werden soll.

  Folgende Alternativen stehen zur Auswahl:

  – *No change*: Es wird erneut vom selben Speichermedium gebootet.
  – *PXE/iSCSI*: Es wird über das Netz von PXE / iSCSI gebootet.
  – *Hard-drive*: Es von der Festplatte gebootet.
  – *CDROM/DVD*: Es wird von CD /DVD gebootet.
  – *Floppy*: Es wird von Floopy Disk gebootet.

- Klicken Sie auf die Schaltfläche *Apply*, um Ihre Einstellungen zu aktivieren.

Power Control - Server ein- und ausschalten

Mit der Gruppe *Power Control* können Sie den Server ein- und ausschalten.

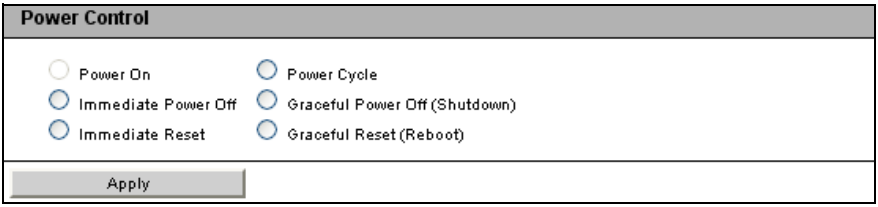


Bild 94: Seite Power On/Off - Power Control

Power On
Schaltet den Server ein.

Immediate Power Off
Schaltet den Server unabhängig vom Status des Betriebssystems aus.

Immediate Reset
Startet den Server unabhängig vom Status des Betriebssystems komplett neu (Kaltstart).

Power Cycle
Schaltet den Server vollständig aus und nach einer konfigurierten Zeit automatisch wieder ein. Diese Zeit können Sie im Eingabefeld *Power Cycle Delay* der Gruppe *ASR&R Options* (siehe Seite 235) konfigurieren.

Graceful Power Off (Shutdown)
Graceful Shutdown und Power Off.
Diese Option ist nur verfügbar, wenn ServerView-Agenten installiert und beim iRMC als „Connected“ gemeldet sind.

Graceful Reset (Reboot)
Graceful Shutdown und Reboot.
Diese Option ist nur verfügbar, wenn ServerView-Agenten installiert und beim iRMC als „Connected“ gemeldet sind.

► Klicken Sie auf die Schaltfläche *Apply,* um die gewünschte Aktion zu starten.

7.6.2 Power Options - Power Management des Servers konfigurieren

Über die Seite *Power Options* können Sie das Verhalten des Servers nach Stromausfall und die Ein-/Ausschaltzeiten des Server festlegen.

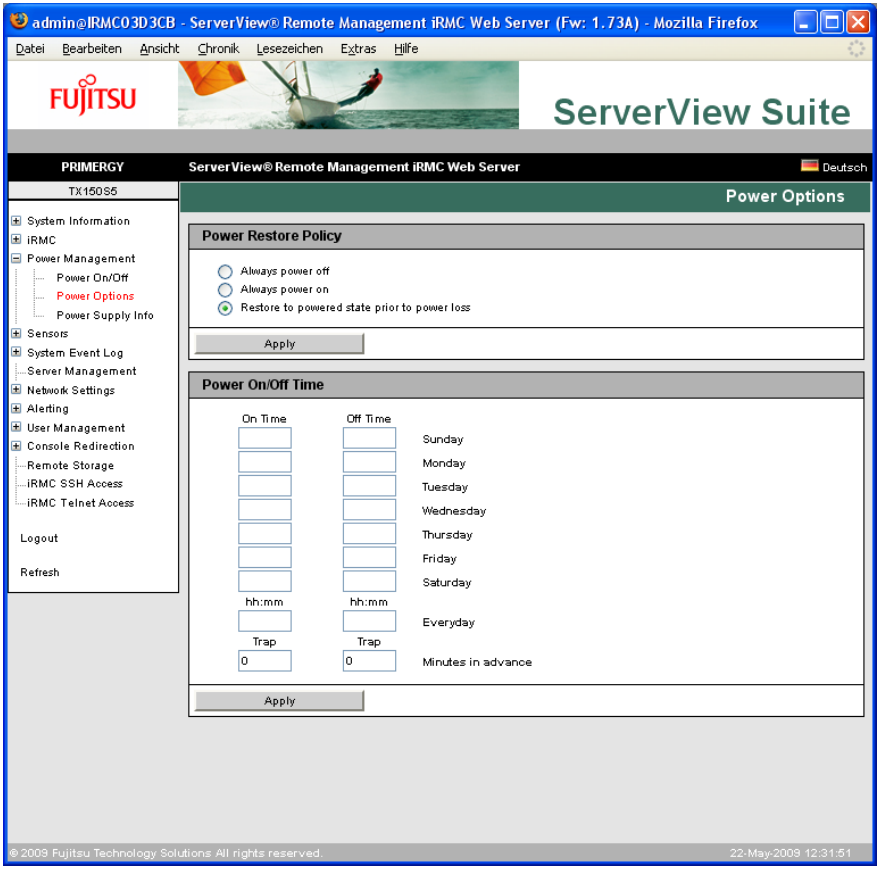


Bild 95: Seite Power Options

Power Restore Policy - Verhalten des Servers nach Stromausfall festlegen

Mit der Gruppe *Power Restore Policy* spezifizieren Sie das Power-Management für den Server nach einem Stromausfall.

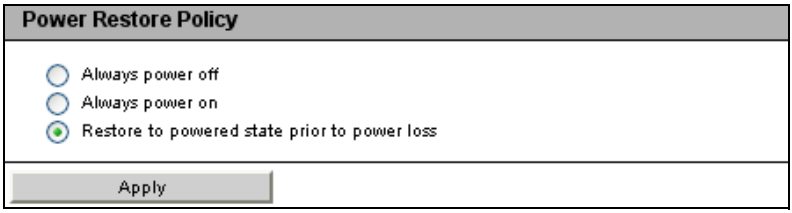


Bild 96: Seite Power Options - Power Restore Policy

Always power off
: Nach Stromausfall bleibt der Server immer ausgeschaltet.

Always power on
: Nach Stromausfall wird der Server jedesmal wieder eingeschaltet.

Restore to powered state prior to power loss
: Power-Status des Servers wird auf den Power-Status vor dem Stromausfall gesetzt.

► Klicken Sie auf die Schaltfläche *Apply*, um Ihre Einstellungen zu aktivieren.

Die konfigurierte Aktion wird nach einem Stromausfall ausgeführt.

Power On/Off Time - Ein-/Ausschalt-Zeiten des Servers festlegen

In den Eingabefeldern der Gruppe *PowerOn/Off Time* spezifizieren Sie die Ein-/Ausschalt-Zeiten des Servers an den einzelnen Wochentagen bzw. die täglichen Ein-/Ausschalt-Zeiten des Servers.

Die Angaben im Eingabefeld *Everyday* haben Vorrang!

Außerdem können Sie in den Feldern *Trap* festlegen, ob und gegebenenfalls wieviele Minuten vor einem geplanten Ein-/Ausschalten des verwalteten Servers der iRMC einen SNMP-Trap an die Management-Konsole senden soll. Wenn Sie den Wert „0“ angeben, werden keine Traps gesendet.

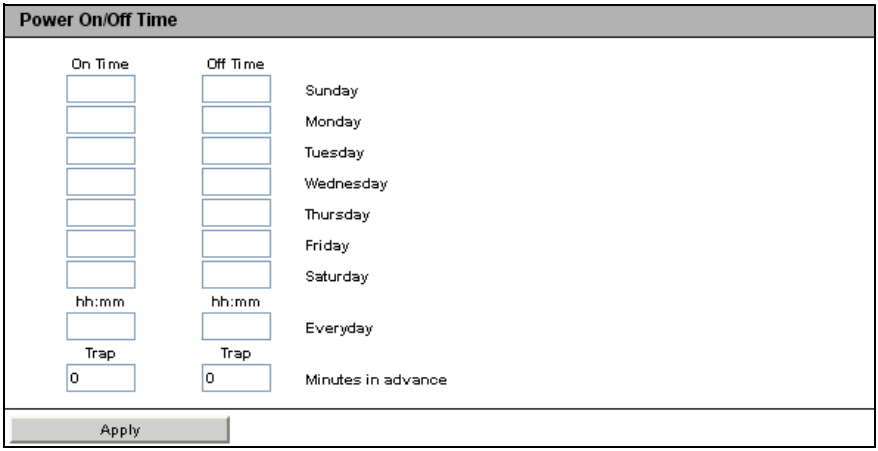
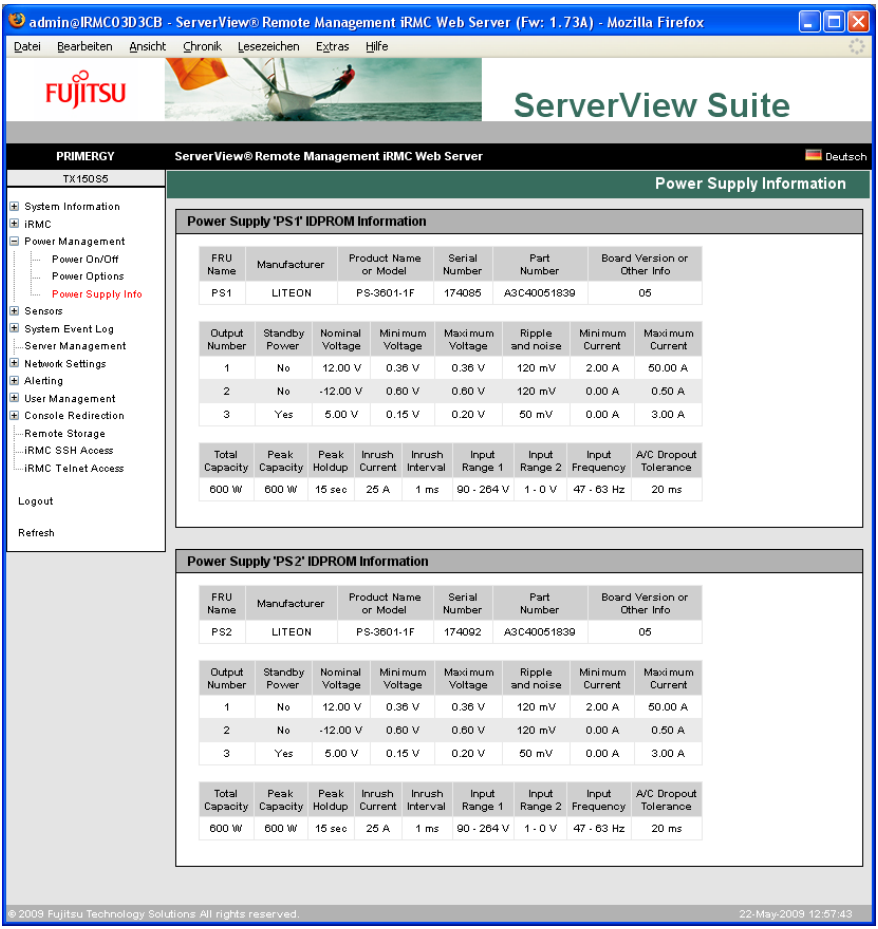


Bild 97: Seite Power Options - Power On/Off Time

► Klicken Sie auf die Schaltfläche *Apply,* um Ihre Einstellungen zu aktivieren.

7.6.3 Power Supply Info - Stromversorgung und IDPROM-Daten der FRU-Komponenten

Auf Seite *Power Supply Info* können Sie sich über die Spezifikationen für die Stromversorgung sowie über die IDPROM-Daten der FRUs des Servers informieren.


admin@IRMC03D3CB - ServerView® Remote Management iRMC Web Server (Fw: 1.73A) - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
FUJITSU
ServerView Suite
PRIMERGY
ServerView® Remote Management iRMC Web Server
Deutsch
TX150S5
System Information
iRMC
Power Management
Power On/Off
Power Options
Power Supply Info
Sensors
System Event Log
Server Management
Network Settings
Alerting
User Management
Console Redirection
Remote Storage
iRMC SSH Access
iRMC Telnet Access
Logout
Refresh
Power Supply Information
Power Supply 'PS1' IDPROM Information
FRU Name | Manufacturer | Product Name or Model | Serial Number | Part Number | Board Version or Other Info
PS1 | LITEON | PS-3601-1F | 174085 | A3C40051839 | 05
Output Number | Standby Power | Nominal Voltage | Minimum Voltage | Maximum Voltage | Ripple and noise | Minimum Current | Maximum Current
1 | No | 12.00 V | 0.36 V | 0.36 V | 120 mV | 2.00 A | 50.00 A
2 | No | -12.00 V | 0.60 V | 0.60 V | 120 mV | 0.00 A | 0.50 A
3 | Yes | 5.00 V | 0.15 V | 0.20 V | 50 mV | 0.00 A | 3.00 A
Total Capacity | Peak Capacity | Peak Holdup | Inrush Current | Inrush Interval | Input Range 1 | Input Range 2 | Input Frequency | A/C Dropout Tolerance
600 W | 600 W | 15 sec | 25 A | 1 ms | 90 - 264 V | 1 - 0 V | 47 - 63 Hz | 20 ms
Power Supply 'PS2' IDPROM Information
FRU Name | Manufacturer | Product Name or Model | Serial Number | Part Number | Board Version or Other Info
PS2 | LITEON | PS-3601-1F | 174092 | A3C40051839 | 05
Output Number | Standby Power | Nominal Voltage | Minimum Voltage | Maximum Voltage | Ripple and noise | Minimum Current | Maximum Current
1 | No | 12.00 V | 0.36 V | 0.36 V | 120 mV | 2.00 A | 50.00 A
2 | No | -12.00 V | 0.60 V | 0.60 V | 120 mV | 0.00 A | 0.50 A
3 | Yes | 5.00 V | 0.15 V | 0.20 V | 50 mV | 0.00 A | 3.00 A
Total Capacity | Peak Capacity | Peak Holdup | Inrush Current | Inrush Interval | Input Range 1 | Input Range 2 | Input Frequency | A/C Dropout Tolerance
600 W | 600 W | 15 sec | 25 A | 1 ms | 90 - 264 V | 1 - 0 V | 47 - 63 Hz | 20 ms
© 2009 Fujitsu Technology Solutions All rights reserved.
22-May-2009 12:57:43
Bild 98: Seite Power Supply Info

7.7 Sensors - Status der Sensoren überprüfen

Unter dem Eintrag „Sensors“ stehen Ihnen Seiten zur Verfügung, mit denen Sie die Sensoren des verwalteten Servers überprüfen können:

– „Fans - Lüfter überprüfen“ auf Seite 220.

– „Temperature - Temperatursensoren überprüfen“ auf Seite 222.

– „Voltages - Spannungssensoren überprüfen“ auf Seite 224.

– „Power Supply - Stromversorgung überprüfen“ auf Seite 225.

– „Component Status - Status der Serverkomponenten überprüfen“ auf Seite 226.

Um die Statusüberprüfung zu erleichtern, wird der Status eines Sensors nicht nur über seinen aktuellen Wert angezeigt, sondern außerdem über Farbcode und Status-Icon:

Schwarz /	Der gemessene Wert liegt innerhalb des im Betriebszustand normalen Wertebereichs.
Orange /	Der gemessene Wert übersteigt die Warnschwelle. Der Systembetrieb ist aber noch nicht gefährdet.
Rot /	Der gemessene Wert übersteigt die kritische Schwelle. Der Systembetrieb kann gefährdet sein und die Datenintegrität könnte bedroht sein.

Tabelle 6: Status der Sensoren

7.7.1 Fans - Lüfter überprüfen

Die Seite *Fans* informiert über Lüfter und deren Status.

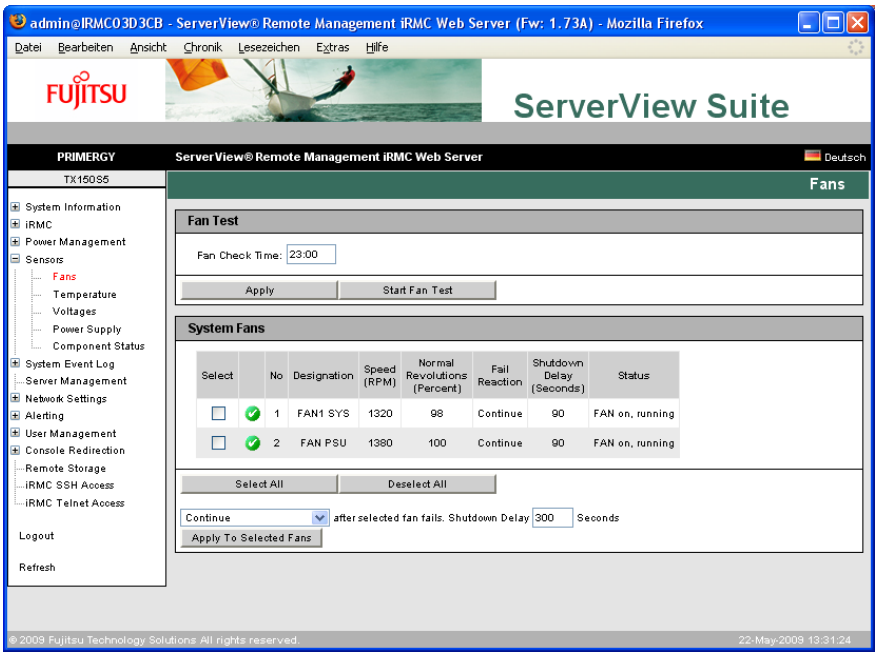


Bild 99: Seite Fans

Fan Test - Lüfter testen

Mit der Gruppe *Fan Test* können Sie einen Zeitpunkt für einen automatischen Start des Lüfter-Tests festlegen oder den Test der Lüfter explizit starten.

Fan Check Time

Tragen Sie hier den Zeitpunkt für einen automatischen Start des Lüfter-Tests ein.

- Klicken Sie auf die Schaltfläche *Apply,* um Ihre Einstellungen zu aktivieren.
- Klicken Sie auf die Schaltfläche *Start Fan Test,* wenn Sie den Lüfter-Test explizit starten wollen.

System Fans - Server-Verhalten bei Ausfall von Lüftern festlegen

Mit der Gruppe *System Fans* können Sie sich über den Status der Lüfter informieren. Dabei können Sie via Option oder Schaltfläche einzelne oder alle Lüfter auswählen und festlegen, ob bei Ausfall dieser Lüfter der Server nach einer spezifizierten Anzahl von Sekunden heruntergefahren werden soll.

Select all
: Alle Lüfter werden ausgewählt.

Deselect all
: Alle Auswahlmarkierungen werden gelöscht.

- ► Markieren Sie die Lüfter, für die Sie ein Verhalten im Fehlerfall definieren wollen.
- ► Definieren Sie das Verhalten im Fehlerfall über die Liste am unteren Ende des Arbeitsbereichs:
  - – Wählen Sie *continue*, wenn bei Ausfall der ausgewählten Lüfter der Shutdown des Servers nicht eingeleitet werden soll.
  - – Wählen Sie *shutdown-and-power-off*, wenn bei Ausfall der ausgewählten Lüfter der Shutdown des Servers eingeleitet und der Server ausgeschaltet werden soll. Spezifizieren Sie in diesem Fall außerdem im Eingabefeld rechts neben der Liste die gewünschten Zeitspanne (Shutdown Delay, in Sekunden) zwischen dem Ausfall des Lüfters und dem Shutdown des Servers.

    i Bei redundanten Lüftern wird der Shutdown erst dann eingeleitet, wenn mehr als ein Lüfter defekt ist und für diese Lüfter außerdem *shutdown-and-power-off* eingestellt ist.
- ► Klicken Sie auf die Schaltfläche *Apply to the selected Fans,* um Ihre Einstellungen für die ausgewählten Lüfter zu aktivieren.

7.7.2 Temperature - Temperatursensoren überprüfen

Die Seite *Temperature* informiert über den Status von Temperatursensoren, die die Temperatur an Serverkomponenten wie z. B CPU oder FBD (Fully buffered DIMM) sowie die Umgebungstemperatur messen.

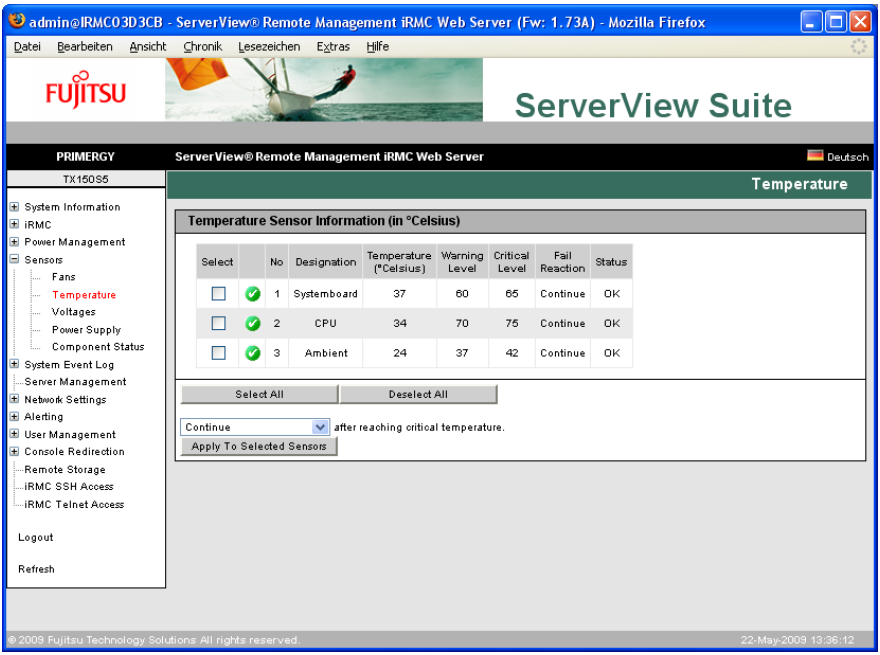


Bild 100: Seite Temperature

Via Option oder Schaltfläche können Sie einzelne oder alle Temperatursensoren auswählen und festlegen, ob bei Erreichen der kritischen Temperatur an den ausgewählten Sensoren der Server heruntergefahren werden soll.

Select all
: Alle Temperatursensoren werden ausgewählt.

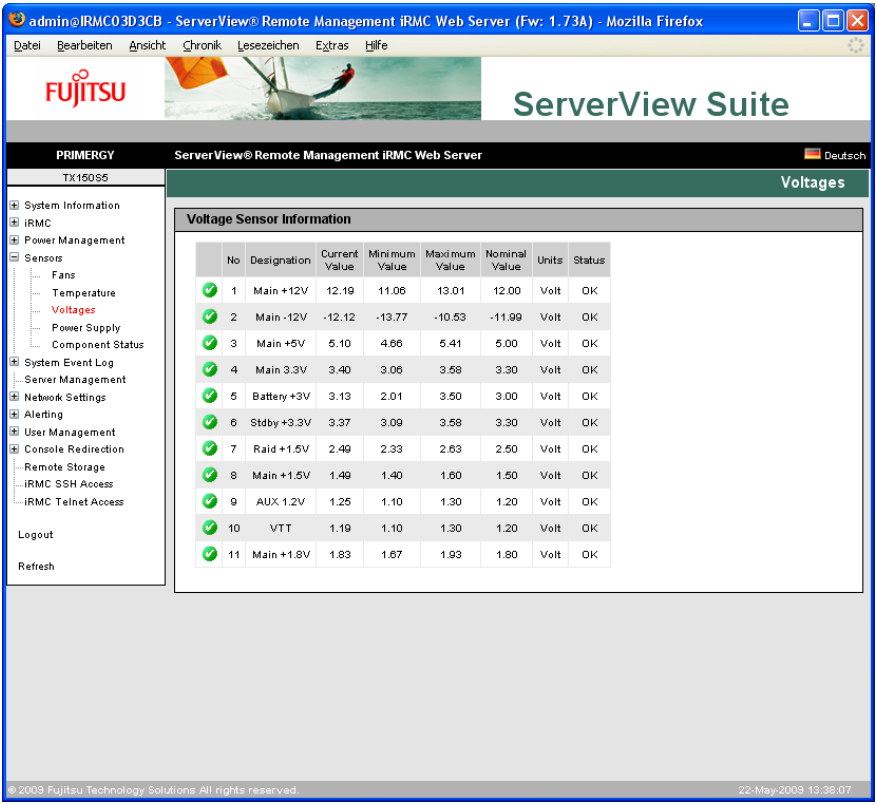
Deselect all
: Alle Auswahlmarkierungen werden gelöscht.

- Markieren Sie die Sensoren, für die Sie ein Verhalten bei Erreichen der kritischen Temperatur definieren wollen.

- Definieren Sie das Verhalten bei Erreichen der kritischen Temperatur über die Liste am unteren Ende des Arbeitsbereichs:
  - Wählen Sie *continue*, wenn bei Erreichen der kritischen Temperatur an den ausgewählten Sensoren der Shutdown des Servers nicht eingeleitet werden soll.
  - Wählen Sie *shutdown-and-power-off*, wenn bei Erreichen der kritischen Temperatur an den ausgewählten Sensoren der Shutdown des Servers eingeleitet und der Server ausgeschaltet werden soll.
- Klicken Sie auf die Schaltfläche *Apply to the selected Sensors,* um Ihre einstellungen für die ausgewählten Temperatursensoren zu aktivieren.

7.7.3 Voltages - Spannungssensoren überprüfen

Die Seite *Voltages* informiert über den Status der Spannungssensoren, die den Server-Komponenten zugeordnet sind.


admin@IRMC03D3CB - ServerView® Remote Management iRMC Web Server (Fw: 1.73A) - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
FUJITSU
ServerView Suite
PRIMERGY
ServerView® Remote Management iRMC Web Server
Deutsch
TX150S5
System Information
iRMC
Power Management
Sensors
Fans
Temperature
Voltages
Power Supply
Component Status
System Event Log
Server Management
Network Settings
Alerting
User Management
Console Redirection
Remote Storage
iRMC SSH Access
iRMC Telnet Access
Logout
Refresh
Voltages
Voltage Sensor Information
No Designation Current Value Minimum Value Maximum Value Nominal Value Units Status
1 Main +12V 12.19 11.06 13.01 12.00 Volt OK
2 Main -12V -12.12 -13.77 -10.53 -11.99 Volt OK
3 Main +5V 5.10 4.66 5.41 5.00 Volt OK
4 Main 3.3V 3.40 3.06 3.58 3.30 Volt OK
5 Battery +3V 3.13 2.01 3.50 3.00 Volt OK
6 Stdby +3.3V 3.37 3.09 3.58 3.30 Volt OK
7 Raid +1.5V 2.49 2.33 2.63 2.50 Volt OK
8 Main +1.5V 1.49 1.40 1.60 1.50 Volt OK
9 AUX 1.2V 1.25 1.10 1.30 1.20 Volt OK
10 VTT 1.19 1.10 1.30 1.20 Volt OK
11 Main +1.8V 1.83 1.67 1.93 1.80 Volt OK
© 2009 Fujitsu Technology Solutions All rights reserved.
22-May-2009 13:38:07
Bild 101: Seite Voltages

7.7.4 Power Supply - Stromversorgung überprüfen

Die Seite *Power Supply* informiert über Stromversorgung durch die Netzgeräte sowie den Stromverbrauch der Systemkomponenten.

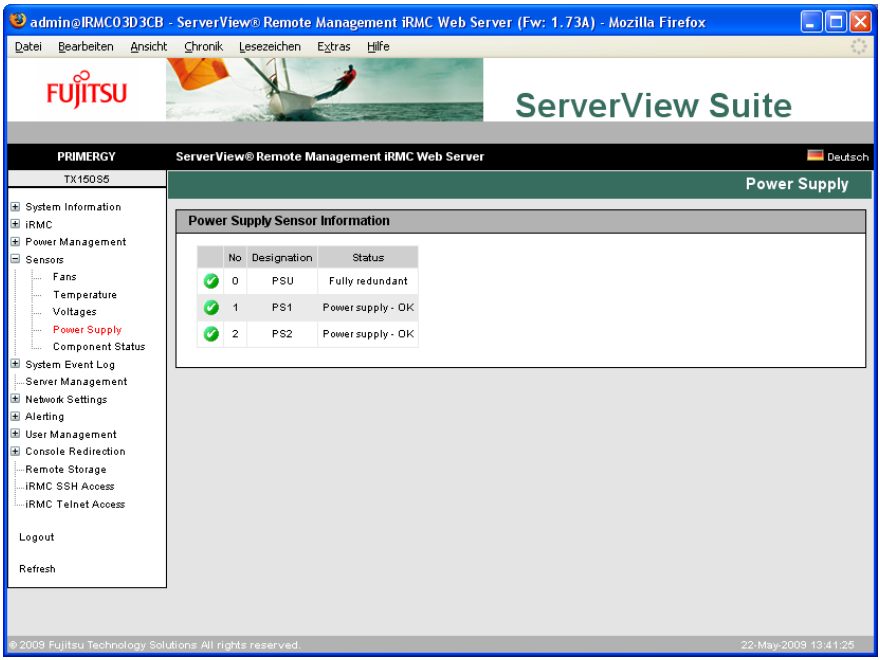


Bild 102: Seite Power Supply

Power Supply Sensor Information

Hier wird der Zustand der Stromversorgung durch die Netzgeräte angezeigt.

7.7.5 Component Status - Status der Serverkomponenten überprüfen

Die Seite *Component Status* informiert über den Status der Serverkomponenten.

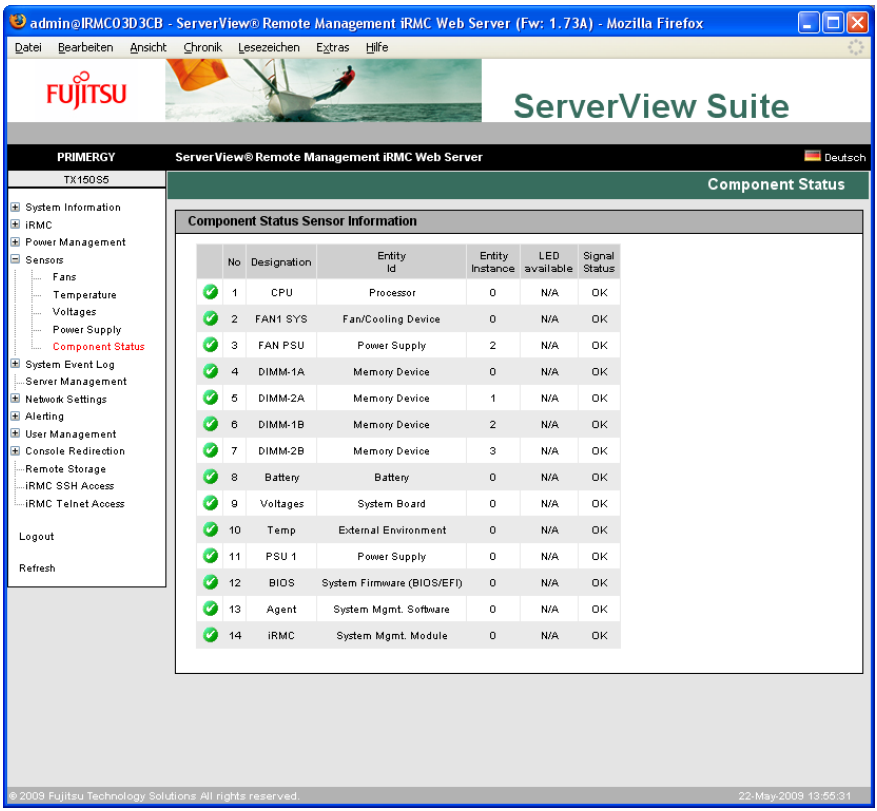

admin@IRMC03D3CB - ServerView® Remote Management iRMC Web Server (Fw: 1.73A) - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
FUJITSU
ServerView Suite
PRIMERGY
ServerView® Remote Management iRMC Web Server
Deutsch
TX150S5
System Information
iRMC
Power Management
Sensors
Fans
Temperature
Voltages
Power Supply
Component Status
System Event Log
Server Management
Network Settings
Alerting
User Management
Console Redirection
Remote Storage
iRMC SSH Access
iRMC Telnet Access
Logout
Refresh
Component Status
Component Status Sensor Information
No Designation Entity Id Entity Instance LED available Signal Status
1 CPU Processor 0 N/A OK
2 FAN1 SYS Fan/Cooling Device 0 N/A OK
3 FAN PSU Power Supply 2 N/A OK
4 DIMM-1A Memory Device 0 N/A OK
5 DIMM-2A Memory Device 1 N/A OK
6 DIMM-1B Memory Device 2 N/A OK
7 DIMM-2B Memory Device 3 N/A OK
8 Battery Battery 0 N/A OK
9 Voltages System Board 0 N/A OK
10 Temp External Environment 0 N/A OK
11 PSU 1 Power Supply 0 N/A OK
12 BIOS System Firmware (BIOS/EFI) 0 N/A OK
13 Agent System Mgmt. Software 0 N/A OK
14 iRMC System Mgmt. Module 0 N/A OK
© 2009 Fujitsu Technology Solutions All rights reserved.
22-May-2009 13:55:31

Bild 103: Seite Component Status

7.8 System Event Log (SEL) - Event-Log des Servers anzeigen und konfigurieren

Der Eintrag *System Event Log* enthält die Links auf die Seiten zur Anzeige und Konfiguration des Eventlog des Servers (System Eventlog, SEL):

– „System Event Log Content - Information zum SEL und SEL-Einträge anzeigen“ auf Seite 228.

– „System Event Log Configuration - SEL konfigurieren“ auf Seite 231.

Zur besseren Übersichtlichkeit sind den einzelnen Ereignis-/Fehlerkategorien farbige Icons zugeordnet:

	Critical
	Major
	Minor
	Informational

Tabelle 7: System Event Log Content - Ereigniskategorien

7.8.1 System Event Log Content - Information zum SEL und SEL-Einträge anzeigen

Die Seite *System Event Log Content* informiert über den SEL und zeigt die SEL-Einträge an.

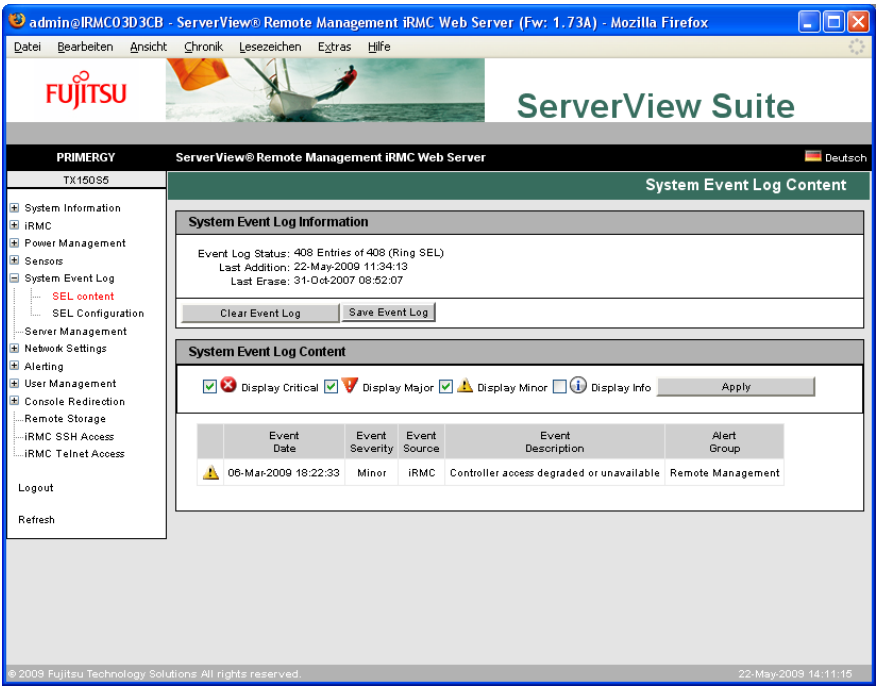


Bild 104: Seite System Event Log Content

System Event Log Information

Die Gruppe *System Event Log Information* informiert über die Anzahl der Einträge im SEL. Außerdem ist vermerkt, wann zuletzt Einträge neu aufgenommen oder gelöscht wurden.

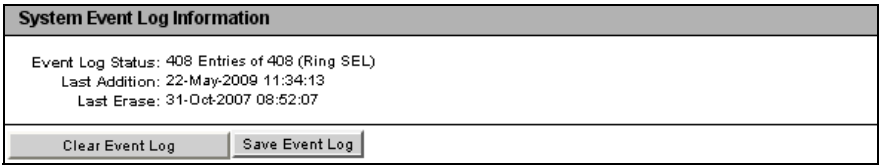

System Event Log Information
Event Log Status: 408 Entries of 408 (Ring SEL)
Last Addition: 22-May-2009 11:34:13
Last Erase: 31-Oct-2007 08:52:07
Clear Event Log
Save Event Log

Bild 105: Seite System Event Log Content - System Event Log Information

Clear Event Log

Durch Klicken auf die Schaltfläche *Clear Event Log* löschen Sie alle Einträge im SEL.

Save Event Log

Nach dem Klicken auf die Schaltfläche *Save Event Log* bietet Ihnen der iRMC die Datei *iRMC_EventLog.sel*, in der die SEL-Einträge gespeichert sind, zum Herunterladen an.

System Event Log Content

In der Gruppe *System Event Log Content* werden die SEL-Einträge nach Fehlerkategorien gefiltert angezeigt.

In der Gruppe *System Event Log Content* können Sie die Filterkriterien für die Dauer der aktuellen Session modifizieren. Die hier vorgenommenen Einstellungen sind jedoch nur bis zum nächsten Logout wirksam. Danach gelten wieder die Standardeinstellungen.

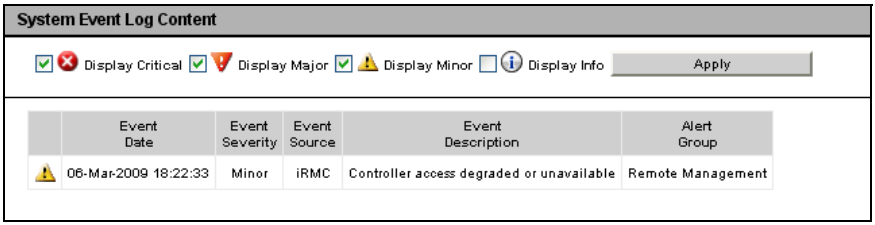


Bild 106: Seite System Event Log Content - System Event Log Content

Display Critical, *Display Major*, *Display Minor*, *Display Info*
Wählen Sie hier gegebenenfalls ein oder mehrere, von der Standardkonfiguration abweichende Fehlerkategorien aus.

- Klicken Sie auf die Schaltfläche *Apply*, um Ihre Einstellungen für die Dauer der aktuellen Session zu aktivieren.

7.8.2 System Event Log Configuration - SEL konfigurieren

In der Seite *System Event Log Configuration* konfigurieren Sie,

– welche SEL-Einträge in der Seite *System Event Log Content* (siehe Seite 228) standardmäßig angezeigt werden.

– ob der SEL als Ringpuffer oder als linearer Puffer organisiert ist.

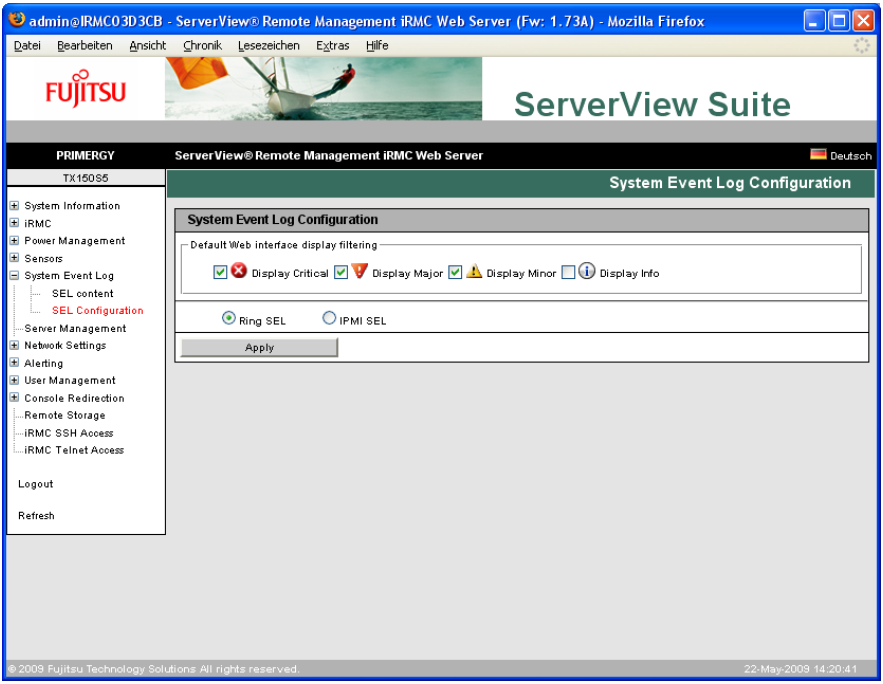


Bild 107: Seite System Event Log Configuration

Default Web interface display filtering

Display Critical, *Display Major*, *Display Minor*, *Display Info*,
Wählen Sie hier ein oder mehrere Fehlerkategorien aus, für die in der Seite *System Event Log Content* standardmäßig die SEL-Einträge angezeigt werden sollen.

> **i** Wenn im verwalteten PRIMERGY Server ein LocalView-Modul eingebaut ist, können Sie zusätzlich die Fehlerkategorien für die Anzeige der SEL-Einträge im Anzeigefeld des LocalView-Moduls auswählen. (Diese Auswahl ist unabhängig von der Auswahl, mit der Sie die in der Seite *System Event Log Content* angezeigten SEL-Einträge festlegen.)

Ring SEL
Der SEL wird als Ringpuffer organisiert.

IPMI SEL
Der SEL wird als linearer Puffer organisiert.

> **i** Wenn der lineare SEL vollständig gefüllt ist, können keine neuen SEL-Einträge mehr aufgenommen werden.

► Klicken Sie auf die Schaltfläche *Apply*, um Ihre Einstellungen zu aktivieren.

7.9 Server Management Information - Server-Einstellungen konfigurieren

Mithilfe der Seite *Server Management Information* können Sie folgende Einstellungen am Server konfigurieren:

– ASR&R-Einstellungen (Automatic Server Reconfiguration and Restart) des Servers (siehe Seite 235)

– Watchdog-Einstellungen (siehe Seite 237)

– Integration von HP System Insight Manager (HP SIM) (siehe Seite 238)

Die auf dieser Seite vorgenommenen Einstellungen sind nach dem nächsten Neustart des verwalteten Servers aktiv.

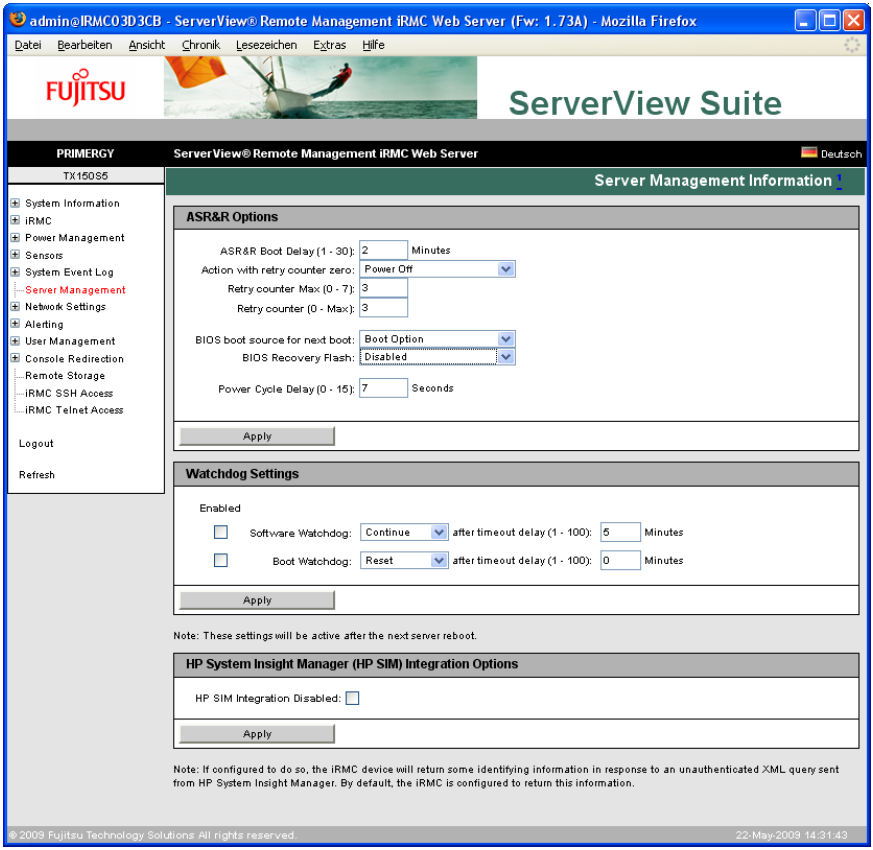

admin@IRMC03D3CB - ServerView® Remote Management iRMC Web Server (Fw: 1.73A) - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
FUJITSU
ServerView Suite
PRIMERGY
ServerView® Remote Management iRMC Web Server
Deutsch
TX150S5
System Information
iRMC
Power Management
Sensors
System Event Log
Server Management
Network Settings
Alerting
User Management
Console Redirection
Remote Storage
iRMC SSH Access
iRMC Telnet Access
Logout
Refresh
Server Management Information
ASR&R Options
ASR&R Boot Delay (1 - 30): 2 Minutes
Action with retry counter zero: Power Off
Retry counter Max (0 - 7): 3
Retry counter (0 - Max): 3
BIOS boot source for next boot: Boot Option
BIOS Recovery Flash: Disabled
Power Cycle Delay (0 - 15): 7 Seconds
Apply
Watchdog Settings
Enabled
Software Watchdog: Continue after timeout delay (1 - 100): 5 Minutes
Boot Watchdog: Reset after timeout delay (1 - 100): 0 Minutes
Apply
Note: These settings will be active after the next server reboot.
HP System Insight Manager (HP SIM) Integration Options
HP SIM Integration Disabled:
Apply
Note: If configured to do so, the iRMC device will return some identifying information in response to an unauthenticated XML query sent from HP System Insight Manager. By default, the iRMC is configured to return this information.
© 2009 Fujitsu Technology Solutions All rights reserved.
22-May-2009 14:31:43

Bild 108: Seite Server Management Information

ASR&R Options - ASR&R-Einstellungen konfigurieren

Mit der Gruppe *ASR&R Options* konfigurieren sie die ASR&R-Einstellungen (Automatic Server Reconfiguration and Restart) des Servers.

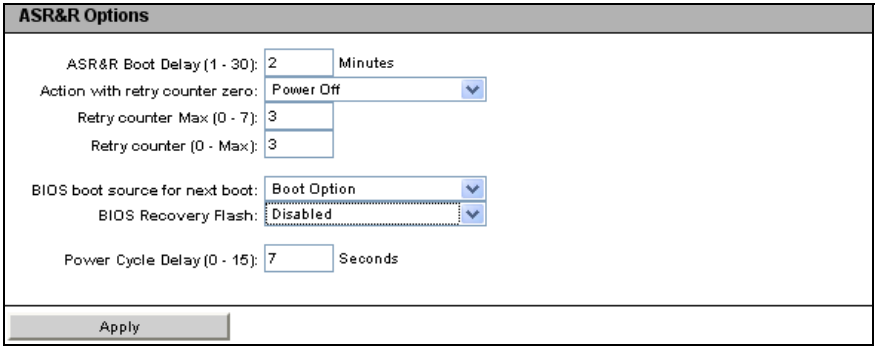


Bild 109: Seite Server Management Information - ASR&R Options

ASR&R Boot Delay

Anzahl an Minuten (max. 30 Min.), die der Server nach einem Shutdown und Power off aufgrund eines kritischen Fehlers wartet, bevor er einen erneuten Boot-Versuch startet.

Action with retry counter zero

Aktion, die durchzuführen ist, nachdem die unter *Retry counter* spezifizierte Anzahl an Neustart-Versuchen fehlgeschlagen ist.

- *Power Off*
  Der Server wird ausgeschaltet.
- *Boot Diagnostic IDE Diskf*
  Es wird von der Diagnostic IDE Disk gebootet.
- *Boot PXE*
  Es wird über das Netz von PXE gebootet.
- *Boot iRMC Remote Image*
  Es wird via Remote Storage vom ServerStart Boot-Image gebootet.
- *Disabled*
  Es wird keine Aktion durchgeführt.

Retry counter Max (0 - 7)

Maximale Anzahl an Neustart-Versuchen, die für den Server nach einem kritischen Fehler möglich sein sollen (max. 7).

Retry counter (0 - Max)
Anzahl an Neustart-Versuchen, die ein Server nach einem kritischen Fehler unternehmen soll (Maximalwert ist der unter *Retry counter Max* eingestellte Wert).

BIOS boot source for next boot
Speichermedium, von dem der nächste Boot des Systems erfolgen soll:

– *Boot Option*
Das System wird von dem auf der Seite *Power On/Off* unter *Boot Options* - *Boot Device Selector* (siehe Seite 213) gewählten Speichermedium gebootet.

– *Diagnostic System*
Es wird das Diagnosesystem gebootet.

BIOS recovery flash bit
Das BIOS Recovery Flash Bit wird aktiviert/deaktiviert:

– *Enabled*
Beim nächsten Booten des Systems wird ein automatischer Flash des BIOS durchgeführt.

– *Disabled*
Beim nächsten Booten des Systems wird kein automatischer Flash des BIOS durchgeführt.

Die Einstellung *Enabled* bietet sich an, wenn nach einem fehlgeschlagenen BIOS-Update das Betriebssystem nicht mehr bootet. Beim nächsten Booten des System von der DOS-Diskette (oder einem DOS-Disketten-Image) wird dann automatisch ein BIOS Recovery Flash durchgeführt.

Setzen Sie nach erfolgtem BIOS Recovery Flash das BIOS Recovery Flash Bit wieder auf *disabled*.

Power Cycle Delay
Zeitspanne (in Sekunden) zwischen Abschalten und Einschalten während eines Powercycle.

► Klicken Sie auf die Schaltfläche *Apply*, um Ihre Einstellungen zu sichern.

Die konfigurierten Einstellungen werden gespeichert und die konfigurierten Aktionen im entsprechenden Fall ausgeführt.

Watchdog Settings - Software Watchdog und Boot Watchdog konfigurieren

Mit der Gruppe *Watchdog Settings* können Sie den Software Watchdog und den Boot Watchdog konfigurieren.

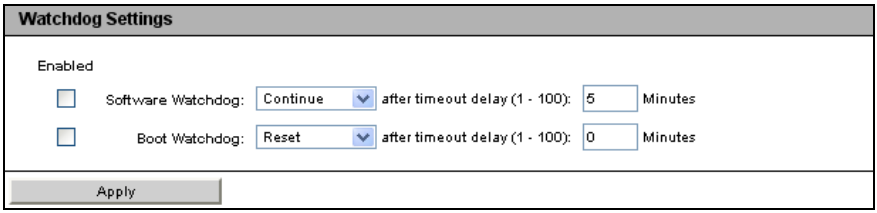


Bild 110: Seite Server Management Information - Watchdog Options

Der **Software Watchdog** überwacht die Arbeit des Systems mithilfe der ServerView-Agenten. Wenn die ServerView-Agenten und das Betriebssystem vollständig initialisiert sind, wird der Software Watchdog aktiviert.
Die ServerView-Agenten kontaktieren in festgelegten Intervallen den iRMC. Laufen von einem ServerView-Agenten keine Meldungen mehr ein, wird daraus geschlossen, dass das System nicht mehr ordnungsgemäß läuft.
Für diesen Fall können Sie eine Aktion festlegen.

Der **Boot Watchdog** überwacht die Phase zwischen dem Systemstart und dem Zeitpunkt, zu dem die ServerView-Agenten zur Verfügung stehen.
Wenn die ServerView-Agenten nicht innerhalb eines festgelegten Zeitraums eine Verbindung zum iRMC des Servers aufbauen, wird daraus geschlossen, dass der Bootvorgang nicht erfolgreich verlaufen ist.
Für diesen Fall können Sie eine Aktion festlegen.

Gehen Sie wie folgt vor:

- Aktivieren/Deaktivieren Sie unter *Enabled* die Option(en) *Software Watchdog* und/oder *Boot Watchdog*.
- Wenn Sie ihn aktiviert haben, konfigurieren Sie hinter *Software Watchdog* und/oder hinter *Boot Watchdog* folgende Einstellungen:

  Continue
  Es wird keine Aktion ausgeführt, wenn der Watchdog abgelaufen ist, d.h. der Server läuft weiter. Ein Event-Log-Eintrag wird erzeugt.

  Reset
  Die Servermanagement-Software löst einen System-Reset aus.

Power Cycle
Der Server wird ausgeschaltet und sofort wieder eingeschaltet.

- Geben Sie nach *after timeout delay* die Zeitspanne (in Minuten) an, nach deren Verstreichen diese Aktion ausgeführt werden soll.

  Der Boot-Watchdog muss solange warten, bis das System gestartet ist. Vereinbaren Sie deshalb für *after timeout delay (1 - 100)* eine hinreichend große Zeitspanne.

- Klicken Sie auf die Schaltfläche *Apply*.

  Die konfigurierten Einstellungen werden gespeichert und die konfigurierten Aktionen im entsprechenden Fall ausgeführt.

HP System Insight Manager (HP SIM) Integrations Options - HP SIM-Integration konfigurieren

Mit der Gruppe *HP System Insight Manager (HP SIM) Integrations Options* legen Sie fest, ob der iRMC als Antwort auf eine nicht authentisierte XML-Anfrage des HP Insight Managers Identifizierungsinformationen an diesen zurücksendet.

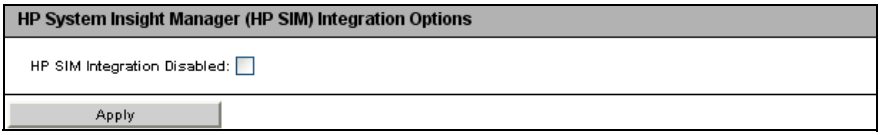


Bild 111: Seite Server Management Information - HP SIM Integrations Options

Gehen Sie wie folgt vor:

- Aktivieren/deaktivieren Sie die Option *HP SIM Integration Disabled*, um die HP SIM-Integration zu deaktivieren bzw. zu aktivieren.
- Klicken Sie auf die Schaltfläche *Apply*, um die gewählte Einstellung zu aktivieren.

7.10 Network Settings - LAN-Parameter konfigurieren

Der Eintrag *Network Settings* umfasst die Links auf die Seiten, mit denen Sie die LAN-Parameter des iRMC konfigurieren:

– „Network Interface - Ethernet-Einstellungen des iRMC konfigurieren“ auf Seite 240.

– „Ports and Network Services - Ports und Netzdienste konfigurieren“ auf Seite 243.

– „DHCP Configuration - Host-Namen für den iRMC konfigurieren“ auf Seite 247.

– „DNS Configuration - DNS für den iRMC aktivieren“ auf Seite 249.

7.10.1 Network Interface - Ethernet-Einstellungen des iRMC konfigurieren

Mit der Seite *Network Interface* können Sie die Ethernet-Einstellungen des iRMC einsehen und ändern.

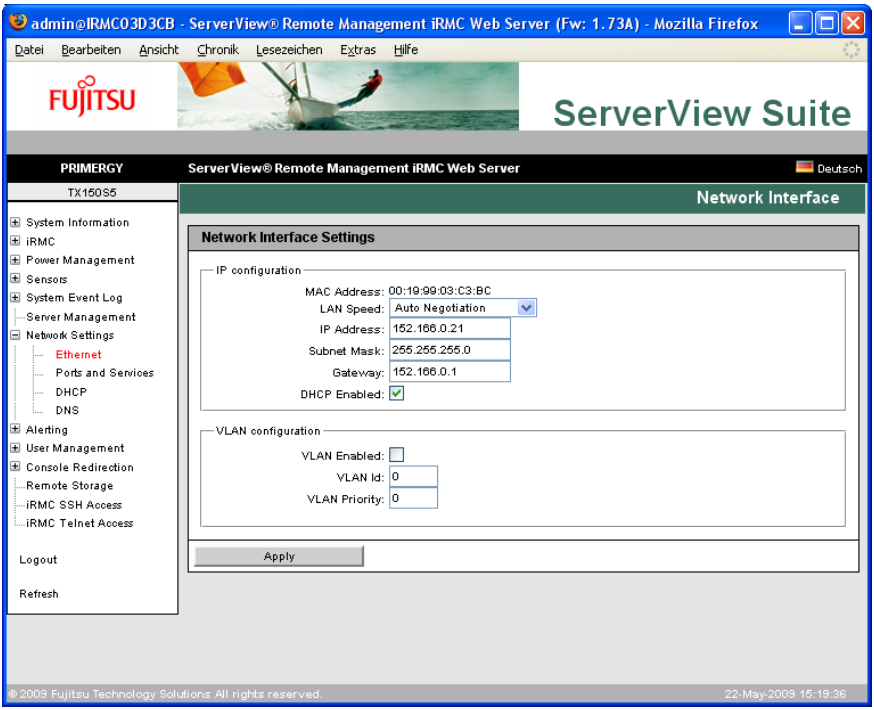


Bild 112: Seite Network Interface

ACHTUNG!

Kontaktieren Sie den zuständigen Netz-Administrator, bevor Sie Ethernet-Einstellungen ändern.

Wenn Sie für den iRMC unzulässige Ethernet-Einstellungen konfigurieren, können Sie nur über eine Konfigurationssoftware, über die serielle Schnittstelle oder im BIOS wieder auf den iRMC zugreifen.

Nur Benutzer mit der Berechtigung *Configure iRMC Settings* können Ethernet-Einstellungen editieren (siehe Kapitel „Benutzerverwaltung für den iRMC“ auf Seite 59).

MAC Address

Hier wird die MAC-Adresse des iRMC angezeigt.

LAN Speed

LAN-Geschwindigkeit. Zur Auswahl stehen:

- Auto Negotiation
- 100 MBit/s Full Duplex
- 100 MBit/s Half Duplex
- 10 MBit/s Full Duplex
- 10 MBit/s Half Duplex

Bei *Auto Negotiation* ermittelt der dem iRMC zugeordnete onboard LAN-Controller selbstständig die korrekte Übertragungsgeschwindigkeit und das Duplex-Verfahren des Netzwerkports, an den er angeschlossen ist.

LAN Port

Diese Option wird nicht für alle PRIMERGY Server unterstützt.

Bei einigen PRIMERGY-Server-Modellen kann die LAN-Schnittstelle der eingebauten System-NIC (Network Interface Card) wahlweise eingerichtet werden als

- *Shared LAN* für den „Shared“-Betrieb mit dem System

  oder als

- *Service LAN* exklusiv für das Management LAN.

Für PRIMERGY Server des Typs TX150 S6 ist die Einstellung *Service LAN* zwingend erforderlich.

IP Address

IP-Adresse des iRMC im LAN. Diese Adresse unterscheidet sich von der IP-Adresse des verwalteten Servers.

Falls mit einer statischen Adresse gearbeitet wird (Option *DHCP enable* nicht aktiviert), können Sie diese hier eingeben. Andernfalls (Option *DHCP enable* aktiviert) verwendet der iRMC das Feld nur zur Anzeige.

Subet Mask

Subnet-Maske des iRMC im LAN.

Gateway

IP-Adresse des Default-Gateway für das LAN.

DHCP Enabled

Wenn Sie diese Option aktivieren, erfragt der iRMC seine LAN-Einstellungen von einem DHCP-Server im Netz.

Aktivieren Sie die Option *DHCP* nicht, wenn im Netz kein DHCP-Server verfügbar ist.
Wenn Sie die Option *DHCP* aktivieren und im Netz kein DHCP-Server verfügbar ist, läuft der iRMC in eine Such-Schleife (d.h. er sucht so lange nach einem DHCP-Server, bis er einen findet).

Der (konfigurierte) iRMC kann von einem entsprechend konfigurierten DHCP-Server bei einem DNS-Server registriert werden (siehe Abschnitte „DHCP Configuration - Host-Namen für den iRMC konfigurieren“ auf Seite 247 und „DNS Configuration - DNS für den iRMC aktivieren“ auf Seite 249).

VLAN Enabled

Mithilfe dieser Option aktivieren Sie die VLAN-Unterstützung für den iRMC.

VLAN Id

VLAN-Identifier des virtuellen Netzes (VLAN), dem der iRMC angehört.
Zulässiger Wertebereich: 1 ≤ *VLAN Id* ≤ 4094.

VLAN Priority

VLAN-Priorität (Benutzerpriorität) des iRMC in dem durch *VLAN Id* spezifizierten VLAN.
Zulässiger Wertebereich: 0 ≤ *VLAN Priority* ≤ 7 (Standardwert: 0).

► Klicken Sie auf die Schaltfläche *Apply*, um die konfigurierten Ethernet-Einstellungen zu aktivieren.

7.10.2 Ports and Network Services - Ports und Netzdienste konfigurieren

Mit der Seite *Ports and Network Services* können Sie die Konfigurationseinstellungen für die Ports und Netzdienste einsehen und ändern.

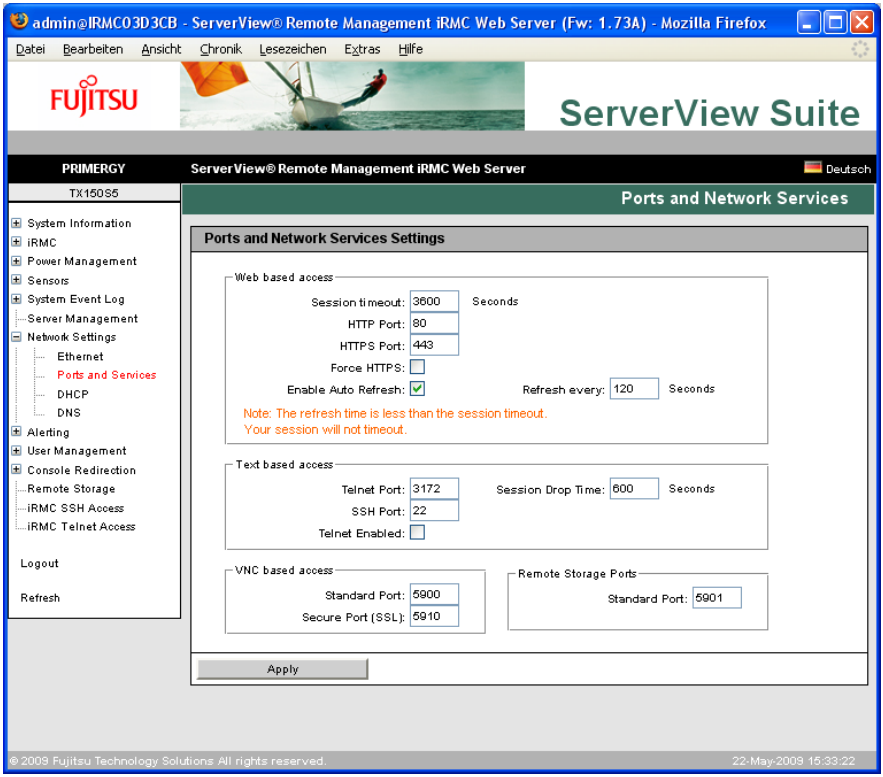


Bild 113: Seite Ports and Network Services

Für Ports, deren Eingabefelder an der iRMC-Web-Oberfläche deaktiviert sind, wird eine Konfiguration nicht unterstützt.

Ports für Web-basierten Zugriff

Session Timeout

Zeitspanne (in Sekunden), nach deren Verstreichen die Session bei Inaktivität automatisch beendet wird. Es wird dann die Login-Seite der iRMC-Web-Oberfläche angezeigt, über die Sie sich erneut einloggen können (siehe Seite 182).

Ihre Session wird auch bei Inaktivität nicht automatisch nach Ablauf der bei *Session Timeout* spezifizierten Zeit beendet, wenn Sie im Eingabefeld *Refresh every ... seconds* (siehe Seite 245) das Aktualisierungsintervall kleiner wählen als den Wert für das *Session Timeout*.

HTTP Port

HTTP Port des iRMC
Default-Portnummer: 80
Konfigurierbar: ja
Standardmäßig aktiviert: ja
Kommunikationsrichtung: inbound und outbound

HTTPS Port

HTTPS (HTTP Secure) Port des iRMC
Default-Portnummer: 443
Konfigurierbar: ja
Standardmäßig aktiviert: ja
Kommunikationsrichtung: inbound und outbound

Force HTTPS

Wenn Sie *Force HTTPS* aktivieren, können die Benutzer nur über den im Dialogfeld angegebenen HTTPS-Port eine gesicherte Verbindung zum iRMC aufbauen.

Wenn Sie die Option *Force HTTPS* deaktivieren, können die Benutzer über den im Dialogfeld angegebenen HTTP-Port eine nicht-gesicherte Verbindung zum iRMC aufbauen.

Wenn das SSL-Zertifikat ausgelaufen ist, wird am Browser eine entsprechende Meldung ausgegeben.

Enable Auto Refresh

Wenn Sie diese Option aktivieren, wird die Anzeige der iRMC-Web-Oberfläche automatisch periodisch aktualisiert. Das Aktualisierungsintervall spezifizieren Sie im Eingabefeld *Refresh every ... seconds*.

Refresh every ... Seconds

Länge (in Sekunden) des Intervalls für die automatische Aktualisierung der iRMC-Web-Oberfläche.

> **i** Wenn Sie das Aktualisierungsintervall kleiner wählen als den Wert für das *Session Timeout* (siehe Seite 244), wird Ihre Session auch bei Inaktivität nicht automatisch nach Ablauf der bei *Session Timeout* spezifizierten Zeit beendet.

Ports für Text-basierten Zugriff

Telnet Port

Telnet Port des iRMC
Default-Portnummer: 3172
Konfigurierbar: ja
Standardmäßig aktiviert: nein
Kommunikationsrichtung: inbound und outbound

SSH Port

SSH (Secure Shell) Port des iRMC
Default-Portnummer: 22
Konfigurierbar: ja
Standardmäßig aktiviert: ja
Kommunikationsrichtung: inbound und outbound

Telnet enabled

Wenn Sie *Telnet Enabled* aktivieren, können die Benutzer über den im Dialogfeld angegebenen Telnet-Port eine Verbindung zum iRMC aufbauen.

Session Drop Time

Zeitspanne (in Sekunden), nach deren Verstreichen eine Telnet-Verbindung bei Inaktivität automatisch abgebaut wird.

VNC Ports

Standard Port

VNC Port des iRMC für sichere und ungesicherte Advanced Video Redirection (AVR)
Portnummer: 80
Konfigurierbar: ja
Standardmäßig aktiviert: ja
Kommunikationsrichtung: inbound

Secure Port (SSL)

VNC Port des iRMC für die SSL-gesicherte Übertragung von Maus- und Tastatureingaben bei AVR.
Portnummer: 443
Konfigurierbar: ja
Standardmäßig aktiviert: ja
Kommunikationsrichtung: inbound

Remote Storage Ports

Standard Port

Standard Remote Storage Port des iRMC
Default-Portnummer: 5901
Konfigurierbar: ja
Standardmäßig aktiviert: ja
Kommunikationsrichtung: outbound zum Remote-Arbeitplatz

► Klicken Sie auf die Schaltfläche *Apply*, um die konfigurierten Einstellungen zu speichern.

7.10.3 DHCP Configuration - Host-Namen für den iRMC konfigurieren

Mit der Seite *DHCP Configuration* können Sie einen Host-Namen für den iRMC konfigurieren und somit „Dynamic DNS“ nutzen. Mit „Dynamic DNS“ können DHCP-Server die IP-Adresse und den Systemnamen einer Netzkomponente selbstständig zur besseren Identifikation an DNS-Server weitergeben.

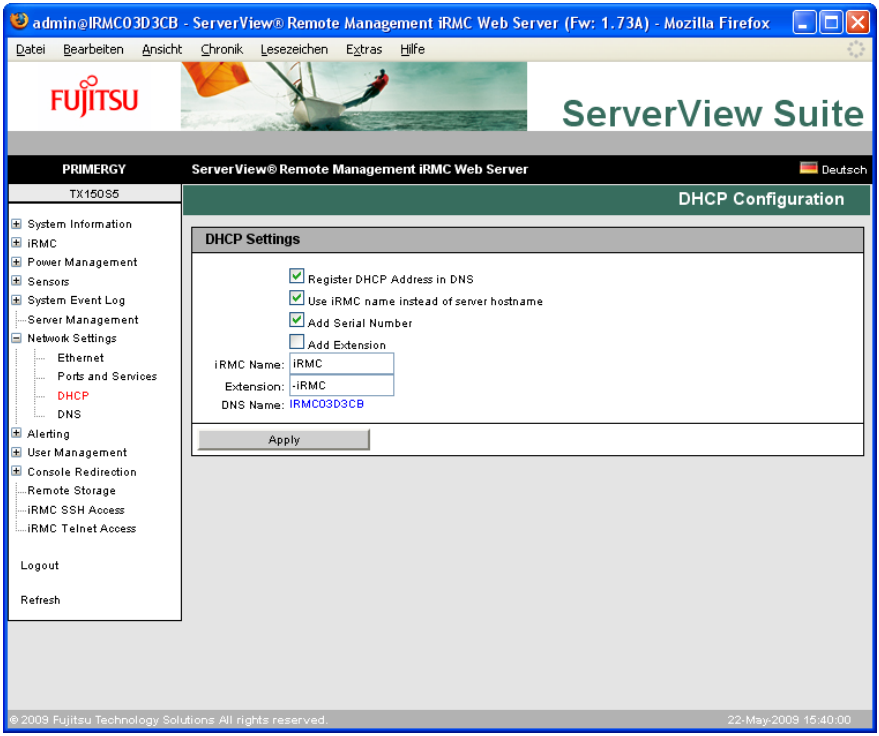


Bild 114: Seite DHCP Configuration

Register DHCP Address in DNS

Aktiviert/ Deaktiviert die DHCP-Namensübergabe für den iRMC an den DHCP-Server.

Use iRMC Name instead of Hostname

Für den iRMC wird der im Dialogfeld *iRMC Name* spezifizierte iRMC-Name anstelle des Servernamens weitergegeben.

Add Serial Number

Dem DHCP-Namen für den iRMC werden die letzten 3 Bytes der MAC-Adresse des iRMC angefügt.

Add Extension

Dem DHCP-Namen für den iRMC wird die im Dialogfeld *Extension* eingetragene Erweiterung angefügt.

Extension

Geben Sie hier eine Namenserweiterung für den iRMC ein.

iRMC Name

iRMC-Name, der für den iRMC anstelle des Servernamens an DHCP weitergegeben wird.

DNS Name

Hier wird der konfigurierte DNS-Name für den iRMC angezeigt.

7.10.4 DNS Configuration - DNS für den iRMC aktivieren

Mit der Seite *DNS Configuration* können Sie für den iRMC den Domain Name Service (DNS) aktivieren. Sie können dann zur Konfiguration des iRMC symbolische DNS-Namen an Stelle von IP-Adressen verwenden.

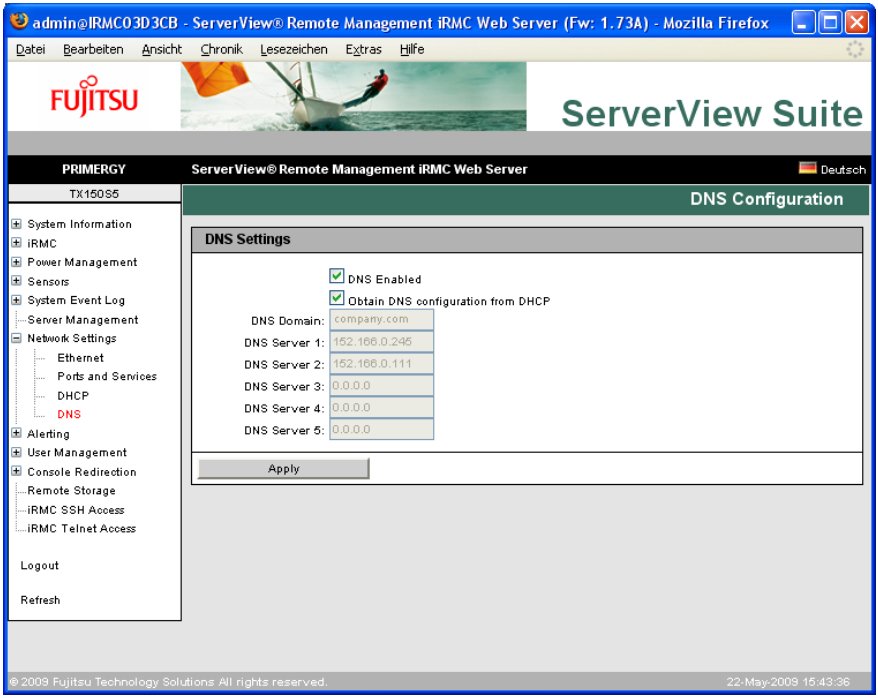


Bild 115: Seite DNS Configuration

DNS Enabled

Aktiviert / Deaktiviert DNS für den iRMC.

Obtain DNS configuration from DHCP

Wenn Sie diese Option aktivieren, werden die IP-Adressen der DNS-Server automatisch vom DHCP-Server übernommen.
In diesem Fall werden bis zu fünf DNS-Server unterstützt.

Wenn Sie diese Einstellung nicht aktivieren, können Sie unter *DNS-Server 1* - *DNS-Server 5* bis zu fünf DNS-Serveradressen manuell eingeben.

DNS Domain

Wenn die Option *Obtain DNS configuration from DHCP* deaktiviert ist, geben Sie hier den Namen der Default-Domäne für Anfragen an den bzw. die DNS Server an.

DNS Server 1 .. 5

Wenn die Option *Obtain DNS configuration from DHCP* deaktiviert ist, können Sie hier die IP-Adressen von bis zu fünf der DNS-Servern angeben.

- Klicken Sie auf die Schaltfläche *Apply*, um die konfigurierten Einstellungen zu speichern.

7.11 Alerting - Alarmbenachrichtigung konfigurieren

Der Eintrag *Alerting* enthält die Links auf die Seiten, mit denen Sie die Alarmbenachrichtigung (Alerting) konfigurieren können:

– „SNMP Trap Alerting - SNMP-Alarmweiterleitung konfigurieren“ auf Seite 252.

– „Serial / Modem Alerting - Alarmweiterleitung über Modem konfigurieren“ auf Seite 254.

– „Email Alerting - E-Mail-Benachrichtigung konfigurieren“ auf Seite 256.

7.11.1 SNMP Trap Alerting - SNMP-Alarmweiterleitung konfigurieren

In der Seite *SNMP Trap Alerting* können Sie die Einstellungen der SNMP-Alarmweiterleitung einsehen und konfigurieren.

Es wird die Weiterleitung von SNMP-Traps an bis zu sieben SNMP-Server unterstützt.

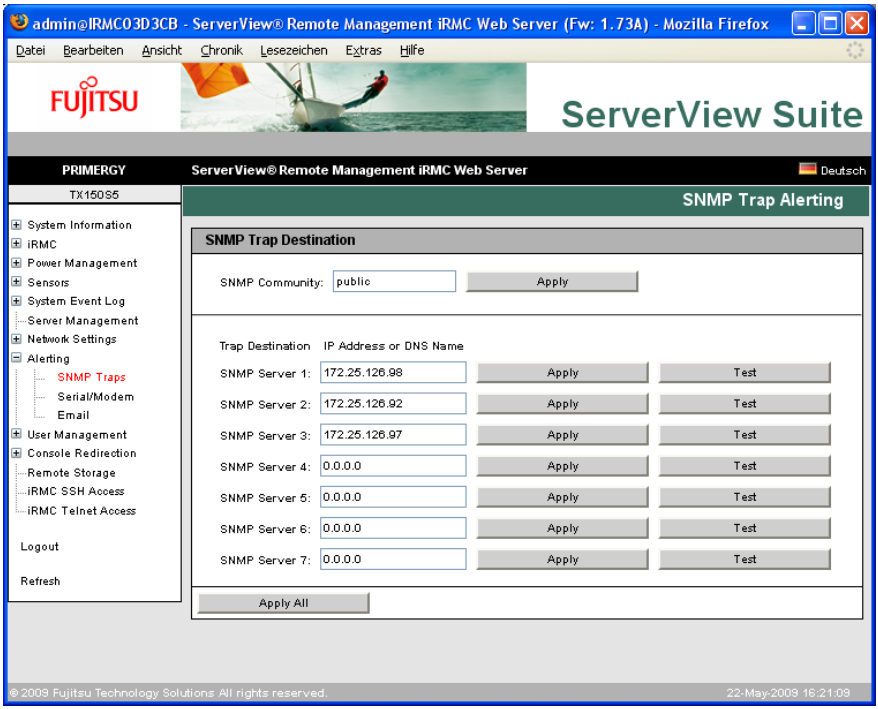


Bild 116: Seite SNMP Trap Alerting

SNMP Community

Name der SNMP-Community.

► Klicken Sie auf die Schaltfläche *Apply*, um den Community-Namen zu übernehmen.

SNMP Server1 .. SNMP Server7 (Trap destinations)
DNS-Namen oder IP-Adressen der Server, die dieser Community angehören und als Trap-Ziele (*Trap Destinations*) konfiguriert werden sollen.

- ► Klicken Sie auf die Schaltfläche *Apply*, um den SNMP Server als Trap-Ziel zu aktivieren.
- ► Klicken Sie auf die Schaltfläche *Test*, um die Verbindung zum SNMP Server zu testen.

► Klicken Sie gegebenenfalls auf die Schaltfläche *Apply All*, um alle Einstellungen zu aktivieren.

7.11.2 Serial / Modem Alerting - Alarmweiterleitung über Modem konfigurieren

Mithilfe der Seite *Serial / Modem Alerting* konfigurieren Sie die Weiterleitung von Alarmen über Modem.

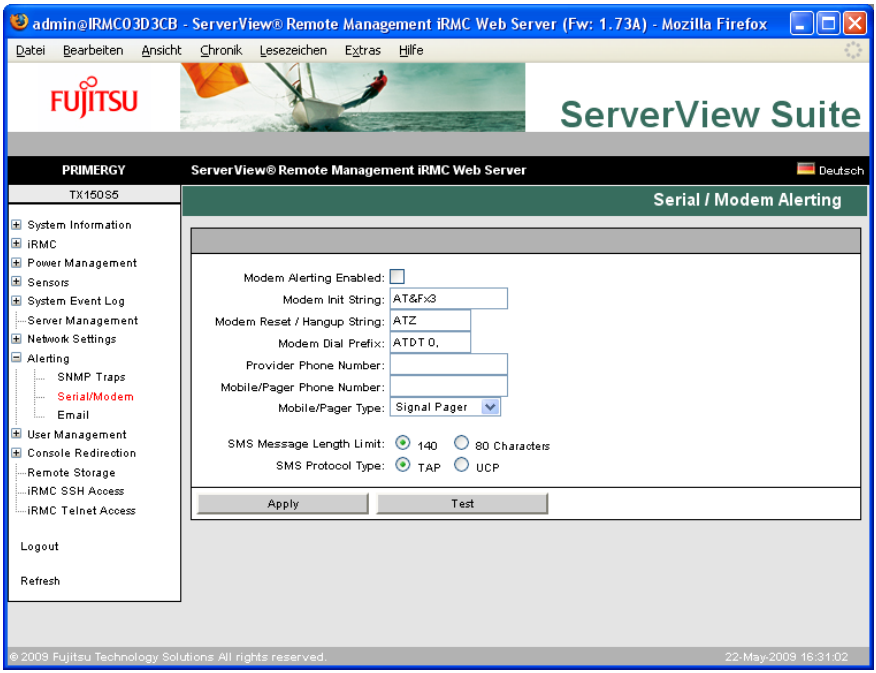


Bild 117: Seite Serial / Modem Alerting

Modem Alerting Enabled

Serial / Modem Alerting wird aktiviert /deaktiviert.

Modem Init String

Entnehmen Sie diese Eingabe der Dokumentation zu Ihrem Modem.

Modem Reset/Hangup String

Entnehmen Sie diese Eingabe der Dokumentation zu Ihrem Modem.

Modem Dial Prefix

Diese Eingabe ist abhängig von der Art des Anschlusses.

Provider Phone Number

Geben Sie die Nummer des SMS-Servers an.

Handy/Pager Phone Number

Geben Sie die Nummer des Mobiltelefons an.

Handy/Pager Type

Hier können Sie wählen zwischen:

- Signal Pager
- Numeric Pager
- Alpha Pager
- SMS
- DoCoMo

SMS Message Length Limit

Als maximale Länge können Sie wahlweise die Werte 80 oder 140 einstellen.

SMS Protocol Type

Aktivieren Sie die Option, die für das genutzte Mobilfunk-Netz steht.

► Klicken Sie auf die Schaltfläche *Apply*, um Ihre Einstellungen zu aktivieren.

► Klicken Sie auf die Schaltfläche *Test*, um einen Test-Alert zu senden.

7.11.3 Email Alerting - E-Mail-Benachrichtigung konfigurieren

Mithilfe der Seite *Email Alerting* konfigurieren Sie die Einstellungen für die E-Mail-Benachrichtigung.

Es wird die Konfiguration von zwei Mail Servern unterstützt.

Email Alerting kann für jeden Benutzer individuell festgelegt werden (siehe Abschnitt „User '<name>' Configuration - Benutzerkonfiguration (Details)“ auf Seite 266).

Email Alerting wird derzeit nicht für globale iRMC-Benutzerkennungen unterstützt (siehe Kapitel „Benutzerverwaltung für den iRMC“ auf Seite 59).

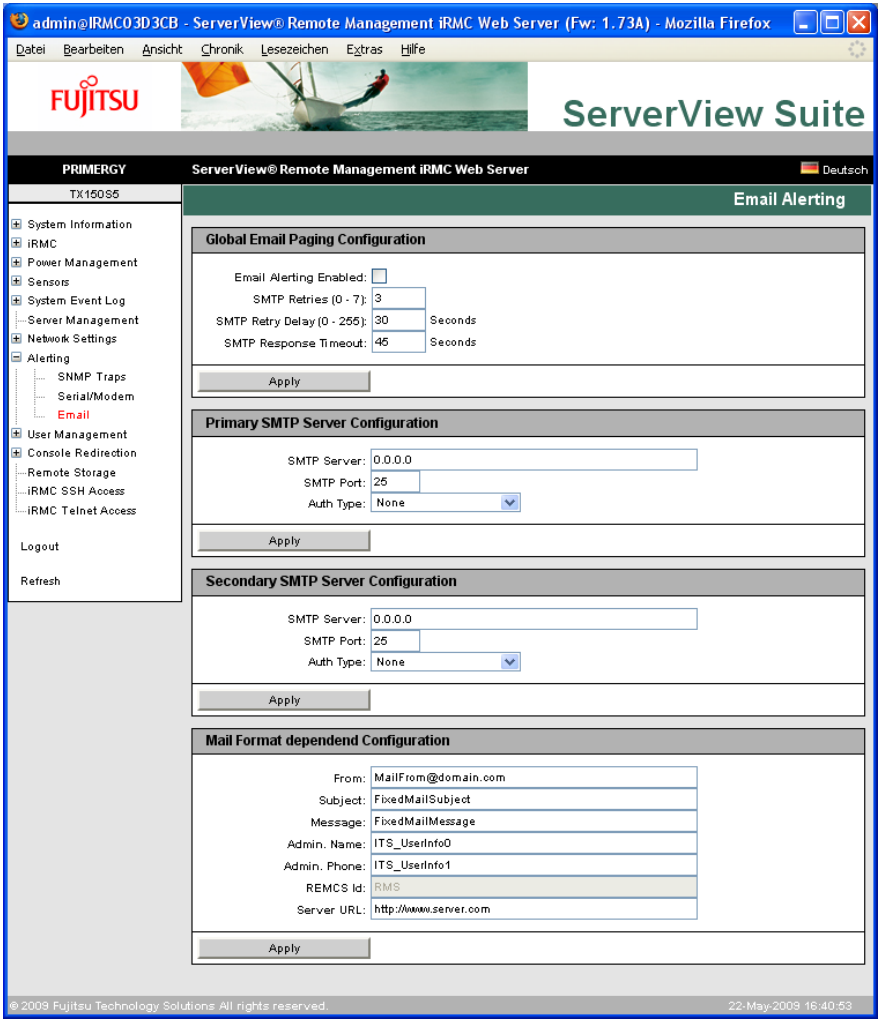


Bild 118: Seite Email Alerting

Global Email Paging Configuration - Globale E-Mail-Einstellungen konfigurieren

Mit der Gruppe *Global Email Paging Configuration* konfigurieren Sie die globalen E-Mail-Einstellungen.

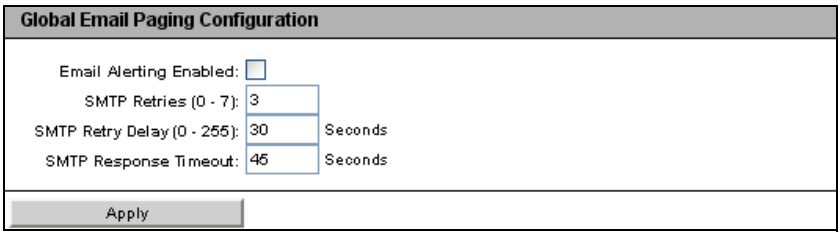


Bild 119: Seite Email Alerting - Global Email Paging Configuration

Email Alerting Enabled
Aktivieren Sie diese Option.

SMTP Retries (0 - 7)
Anzahl der SMTP-Retries.

SMTP Retry Delay (0 - 255)
Zeitspanne (in Sekunden) zwischen den SMTP-Retries.

SMTP Response Timeout
Timeout-Wert (in Sekunden) für SMTP-Antwort.

► Klicken Sie auf die Schaltfläche *Apply*, um Ihre Einstellungen zu aktivieren.

Primary SMTP Server Configuration - Primären Mail Server konfigurieren

Mit der Gruppe *Primary SMTP Server Configuration* konfigurieren Sie den primären Mail Server (SMTP Server).

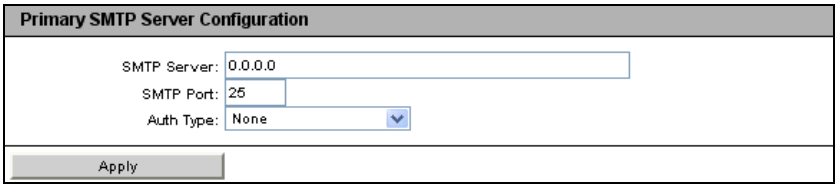


Bild 120: Seite Email Alerting - Primary SMTP Server Configuration

SMTP Server
IP-Adresse des primären Mail Servers.

> Sie können für den iRMC den Domain Name Service (DNS) aktivieren (siehe „DNS Configuration - DNS für den iRMC aktivieren“ auf Seite 249). Anstelle der IP-Adresse können Sie dann einen symbolischen Namen angeben.

SMTP Port
SMTP Port des Mail Servers

Auth Type
Einstellung für die Authentifizierung einer Verbindung des iRMC zum Mail Server:

- *None*
  Keinerlei Authentifizierung der Verbindung.
- *SMTP AUTH (RFC 2554)*
  Authentifizierung nach RFC 2554: SMTP Service Extension for Authentication

Auth User Name
Benutzername für die Authentisierung beim Mail Server

Auth Password
Passwort für die Authentisierung beim Mail Server

Confirm Password
Bestätigen Sie hier Ihr Passwort.

► Klicken Sie auf die Schaltfläche *Apply*, um Ihre Einstellungen zu aktivieren.

Secondary SMTP Server Configuration - Sekundären Mail Server konfigurieren

Mit der Gruppe *Secondary SMTP Server Configuration* konfigurieren Sie den sekundären Mail Server (SMTP Server).

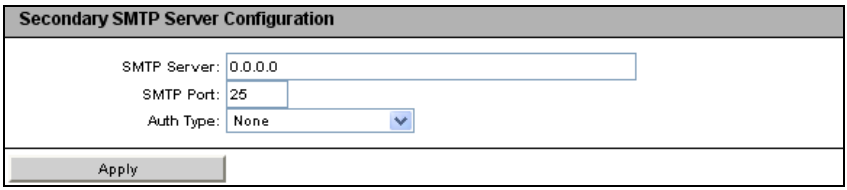


Bild 121: Seite Email Alerting - Secondary SMTP Server Configuration

SMTP Server

IP-Adresse des sekundären Mail Servers.

> Sie können für den iRMC den Domain Name Service (DNS) aktivieren (siehe „DNS Configuration - DNS für den iRMC aktivieren“ auf Seite 249). Anstelle der IP-Adresse können Sie dann einen symbolischen Namen angeben.

SMTP Port

SMTP Port des Mail Servers

- Klicken Sie auf die Schaltfläche *Apply*, um Ihre Einstellungen zu aktivieren.

Mail Format dependend Configuration - Mail-Format-abhängige Einstellungen konfigurieren

Mit der Gruppe *Mail Format dependend Configuration* konfigurieren Sie die vom Mail-Format abhängigen Einstellungen. Das Mail-Format legen Sie pro Benutzer fest mithilfe der Seite *New User Configuration* - *User <Name> Configuration* - *Email Format Configuration* (siehe Seite 270).

Es werden die folgenden Mail-Formate unterstützt:

- Standard
- Fixed Subject
- ITS-Format
- Fujitsu REMCS Format

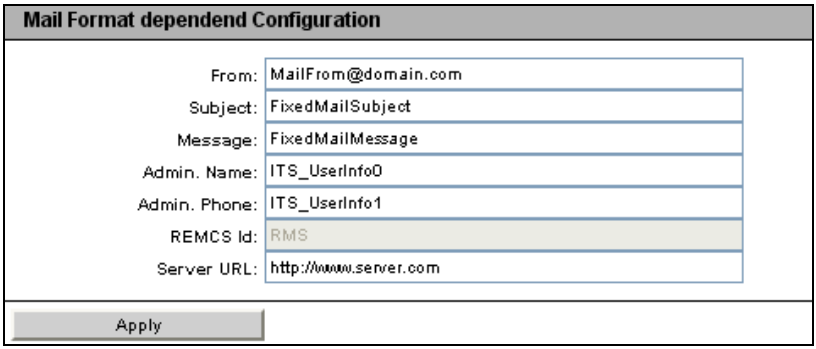


Bild 122: Seite Email Alerting - Mail Format dependend Configuration

Je nach Mail-Format sind nicht alle Eingabefelder aktiv.

From

Identifikation des sendenden iRMC.
Aktiv bei allen Mail-Formaten.

> **i** Wenn in der hier eingegebenen Zeichenfolge ein „@“ enthalten ist, wird diese Zeichenfolge als gültige E-Mail-Adresse interpretiert. Andernfalls wird „admin@<ip-adresse>“ als gültige E-Mail-Adresse verwendet.

Subject

Fixed Subject der Alarmmeldung-E-Mails.
Aktiv nur bei Mail-Format *Fixed Subject* (siehe Seite 270).

Message

Art der Mitteilung (E-Mail).
Aktiv nur bei Mail-Format *Fixed Subject* (siehe Seite 270).

Admin Name

Name des verantwortlichen Administrators (optional).
Aktiv nur bei Mail-Format *ITS* (siehe Seite 270).

Admin Phone

Telefonnummer des verantwortlichen Administrators (optional).
Aktiv nur bei Mail-Format *ITS* (siehe Seite 270).

REMCS Id

Diese ID ist eine zusätzliche Indentifikation des Servers, ähnlich der Seriennummer.
Aktiv nur bei Mail-Format *Fujitsu REMCS-Format*.

Server URL

Eine URL, unter der der Server unter bestimmten Voraussetzungen zugänglich ist. Sie müssen die URL manuell eingeben.
Aktiv nur bei Mail-Format *Standard*.

► Klicken Sie auf die Schaltfläche *Apply,* um Ihre Einstellungen zu speichern.

7.12 User Management - Benutzerverwaltung

Der Eintrag *User Management* enthält die Links auf die Seiten für die lokale Benutzerverwaltung sowie für die Konfiguration des Directory Service für die globale Benutzerverwaltung (LDAP-Konfiguration):

– „iRMC User - lokale Benutzerverwaltung am iRMC“ auf Seite 263

– „Directory Service Configuration (LDAP) - Directory Service am iRMC konfigurieren“ auf Seite 273

7.12.1 iRMC User - lokale Benutzerverwaltung am iRMC

Die Seite *iRMC User* enthält eine tabellarische Übersicht über alle konfigurierten Benutzer: Pro Zeile werden die Daten eines konfigurierten Benutzers dargestellt. Die Benutzernamen sind dabei als Links realisiert. Durch Klicken auf einen Benutzernamen öffnet sich das Fenster *User '<name>' Configuration* (siehe Seite 266), in dem Sie die Einstellungen des betreffenden Benutzers einsehen und/oder modifizieren können.

Die User Id 1 („Null-User“) ist reserviert für den IPMI-Standard und steht deshalb nicht für die Benutzerverwaltung am iRMC zur Verfügung.

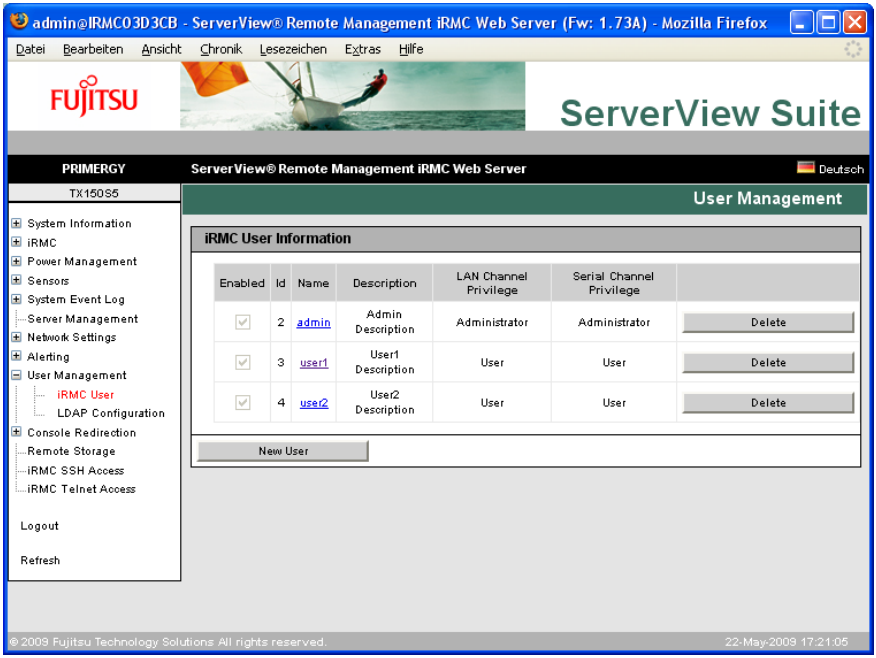


Bild 123: Seite User Management

Delete

In der Tabelle der konfigurierten Benutzer finden Sie hinter jedem Benutzereintrag eine Schaltfläche *Delete*. Durch Klicken auf diese Schaltfläche können Sie den zugehörigen Benutzer nach nochmaliger Bestätigung löschen.

New User

Wenn Sie auf diese Schaltfläche klicken, öffnet sich die Seite *New User Configuration* (siehe Seite 265), über das Sie einen neuen Benutzer konfigurieren können.

7.12.1.1 New User Configuration - Neuen Benutzer konfigurieren

Mithilfe der Seite *New User Configuration* konfigurieren Sie die Grundeinstellungen eines neuen Benutzers.

Erläuterungen zu den Dialogfeldern und Auswahllisten der Seite *New User Configuration* finden Sie ab Seite 267 bei der Beschreibung der Seite *User '<name>' Configuration*.

In Bild 124 ist die Konfiguration eines Benutzers „user3“ dargestellt.

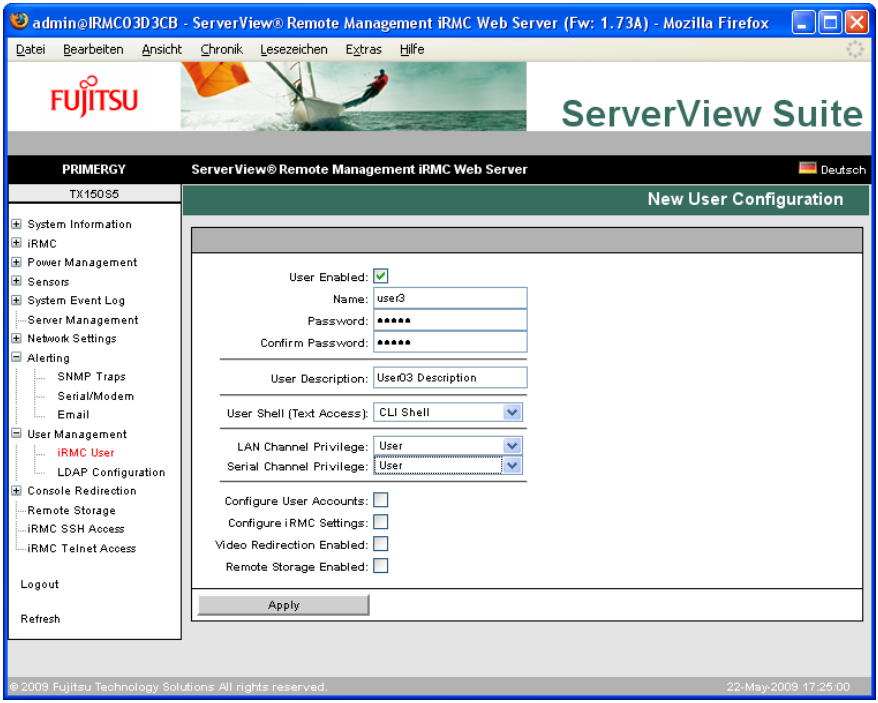


Bild 124: Seite User Management - New User Configuration

7.12.1.2 User '<name>' Configuration - Benutzerkonfiguration (Details)

Mithilfe der Seite *User '<name>' Configuration* können Sie die Einstellungen für einen Benutzer einsehen, ändern und erweitern.

In Bild 125 ist die Konfiguration des in Bild 124 neu angelegten Benutzers dargestellt.

Die User Id wird, in Klammern eingeschlossen, hinter dem Benutzernamen angezeigt.

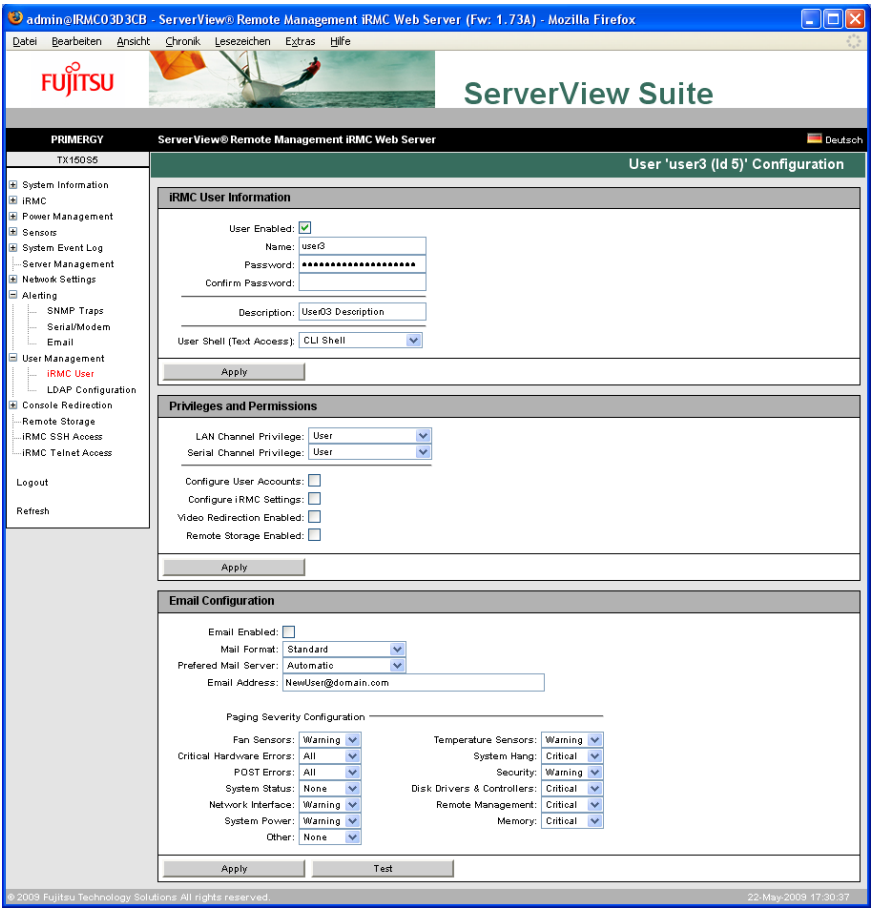


Bild 125: Seite User Management - User '<name>' Configuration

User Information - Zugangsdaten des Benutzers konfigurieren

Mit der Gruppe *User Information* konfigurieren Sie die Zugangsdaten des Benutzers.

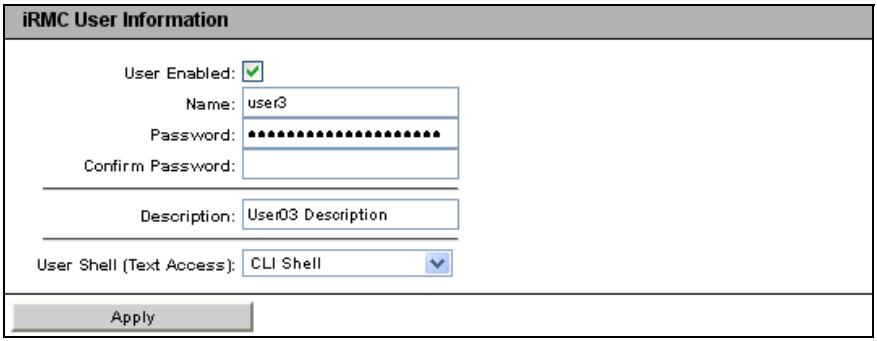


Bild 126: Seite User Management - User '<name>' Configuration - User Information

User Enabled
Durch deaktivieren der Option können Sie den Benutzer sperren.

Name
Tragen Sie hier den Namen des Benutzers ein.

Password
Tragen Sie hier das Passwort des Benutzers ein.

Confirm Password
Wiederholen Sie hier zur Bestätigung die Eingabe des Passworts.

Description
Tragen Sie hier eine allgemeine Beschreibung des konfigurierten Benutzers ein.

User Shell

Wählen Sie hier die gewünschte Benutzer-Shell aus.
Zur Auswahl stehen:

- *SMASH CLP*
  Siehe Abschnitt „Start a Command Line shell... - SMASH CLP Shell starten“ auf Seite 327.
- *CLI Shell*
  Siehe Abschnitt „Command Line Protocol (CLP)“ auf Seite 328.
- *Remote Manager*
  Siehe Kapitel „iRMC über Telnet/SSH (Remote Manager) bedienen“ auf Seite 307.
- *IPMI Basic Mode*
- *IPMI Terminal Mode*
- *None*

► Klicken Sie auf die Schaltfläche *Apply,* um Ihre Einstellungen zu aktivieren.

Privileges and Permissions - Benutzerprivilegien erteilen

Mit der Gruppe *Privileges and Permissions* konfigurieren Sie die Kanal-spezifischen Benutzerprivilegien.

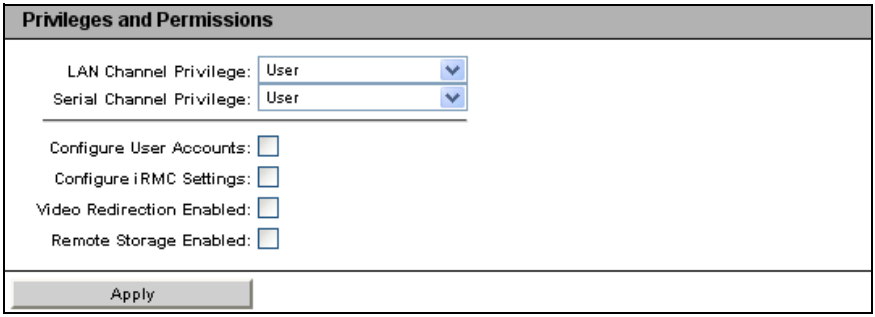


Bild 127: Seite User Management - User '<name>' Configuration - Privileges / Permissions

LAN Channel Privilege

Ordnen Sie hier dem Benutzer eine Berechtigungsgruppe für den LAN-Kanal zu:

- *User*
- *Operator*
- *Administrator*
- *OEM*

Zum Berechtigungsumfang der einzelnen Berechtigungsgruppen siehe Abschnitt „Benutzerberechtigungen“ auf Seite 62.

Serial Channel Privilege

Ordnen Sie hier dem Benutzer eine Berechtigungsgruppe für den seriellen Kanal zu. Zur Auswahl stehen die gleichen Berechtigungsgruppen wie unter *LAN Channel*.

Ergänzend zu den Kanal-spezifischen Berechtigungen können Sie einem Benutzer individuell folgende Kanal-unabhängigen Berechtigungen erteilen:

Configure User Accounts

Berechtigung zum Konfigurieren von lokalen Benutzerzugangsdaten.

Configure iRMC Settings

Berechtigung zum Konfigurieren der iRMC-Einstellungen.

Video Redirection Enabled

Berechtigung zur Nutzung der Advanced Video Redirection (AVR) im „View Only“- und „Full Control“-Modus.

Remote Storage Enabled

Berechtigung zur Nutzung der Remote Storage-Funktionalität.

► Klicken Sie auf die Schaltfläche *Apply,* um Ihre Einstellungen zu aktivieren.

Email Configuration - Benutzer-spezifische E-Mail-Einstellungen konfigurieren

Mit der Gruppe *Email Configuration* konfigurieren Sie die Benutzer-spezifischen Einstellungen für das E-Mail-Format.

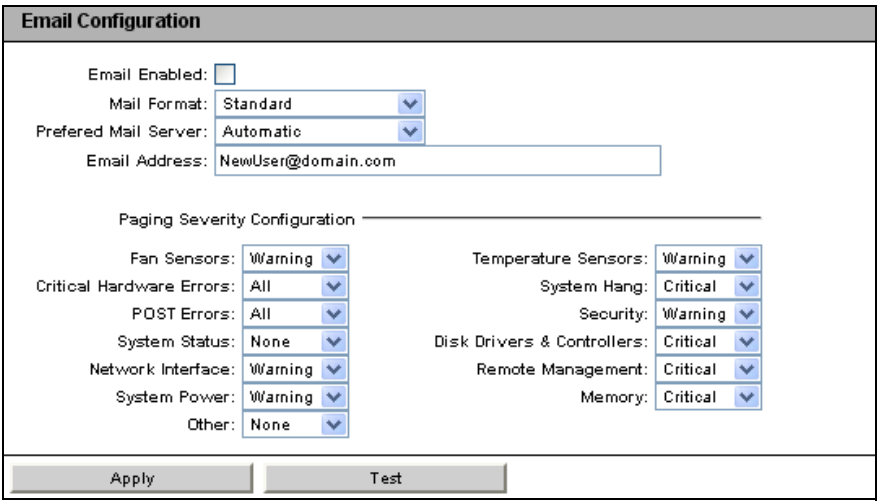


Bild 128: Seite User Management - User ’<name> ’ Configuration - Email Configuration

Email Enabled

Hier stellen Sie ein, ob der Benutzer per E-Mail über die Systemzustände informiert werden soll.

Mail Format

Abhängig vom gewählten Mail-Format können Sie in der Gruppe *Email Alerting - Mail Format dependend Configuration* (siehe Seite 261) unterschiedliche Einstellungen vornehmen.

Folgende Mail-Formate stehen zur Verfügung:

- *Standard*
- *Fixed Subject*
- *ITS-Format*
- *Fujitsu REMCS Format*

Preferred Mail Server

Bevorzugter Mail Server.
Sie können wählen zwischen folgenden Optionen:

- *Automatic*

  Falls die E-Mail nicht sofort erfolgreich versendet werden kann, weil z.B. der erste Mail-Server nicht verfügbar ist, wird E-Mail an den zweiten Mail-Server gesendet.

- *Primary*

  Nur der als Primary SMTP Server (siehe Seite 259) konfigurierte Mail Server wird als bevorzugter Mail Server verwendet.

- *Secondary*

  Nur der als Secondary SMTP Server (siehe Seite 260) konfigurierte Mail Server wird als bevorzugter Mail Server verwendet.

Fehler beim Versenden der E-Mail werden als Event Log gemeldet.

User Description

Allgemeine Beschreibung des konfigurierten Benutzers.

Email Address

E-Mail-Adresse des Empfängers.

Paging Severity Configuration

Hier können Sie Systemereignisse konfigurieren, über die ein iRMC-Benutzer per E-Mail benachrichtigt werden soll.

Jeder Event-Log-Eintrag des iRMC wird einer bestimmten Paging-Gruppe zugeordnet.

Für jede Ereignisgruppe sind folgende Einstellungen möglich:

None

Die Benachrichtigungsfunktion für diese Paging-Gruppe ist deaktiviert.

Critical

Der iRMC benachrichtigt Benutzer per E-Mail, wenn ein System-Event-Log-Eintrag den Status *Citical* meldet.

Warning

Der iRMC benachrichtigt Benutzer per E-Mail, wenn ein System-Event-Log-Eintrag ein Ereignis der Klassen *Minor*, *Major* oder *Critical* meldet.

Unter der Einstellung *WARNING* werden dem Benutzer zusätzlich auch System-Event-Log-Einträge mit dem Status *CRITICAL* gemeldet.

All

Der iRMC benachrichtigt Benutzer über jedes zu einem Eintrag in den System Event-Log führende Ereignis in dieser Gruppe.

► Klicken Sie auf die Schaltfläche *Apply,* um Ihre Einstellungen zu aktivieren.

7.12.2 Directory Service Configuration (LDAP) - Directory Service am iRMC konfigurieren

Für die globale Benutzerverwaltung über einen Directory Service (siehe Seite 68) müssen Sie den iRMC mithilfe der Seite *Directory Service Configuration* entsprechend konfigurieren.

Derzeit werden LDAP-Zugriffe des iRMC für die Directory Services Microsoft Active Directory, Novell eDirectory und Open LDAP unterstützt.

Die folgenden Zeichen sind in LDAP als Meta-Zeichen für Such-Strings reserviert: &, |, !, =, <, >, ~, :

Verwenden Sie diese Zeichen deshalb nicht als Bestandteil von Relative Distinguished Names (RDN).

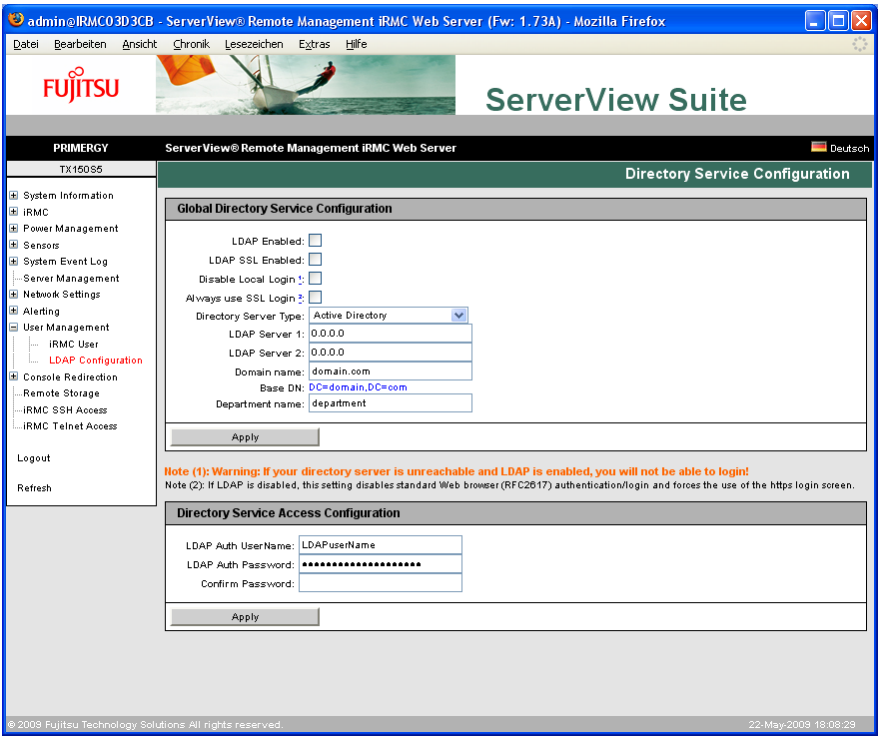


Bild 129: Seite Directory Service Configuration (LDAP-Konfiguration)

Global Directory Service Configuration: Allgemeine Angaben

In der Gruppe *Global Directory Service Configuration* konfigurieren Sie den LDAP-Zugriff des iRMC auf den Directory Service.

LDAP Enabled

Mit dieser Option legen Sie fest, ob der iRMC via LDAP auf einen Directory Service zugreifen kann. Der Directory Service via LDAP kann nur genutzt werden, wenn *LDAP Enable* aktiviert ist.

Wenn *LDAP Enable* aktiviert ist, wird die Login-Information (siehe Seite 182) immer SSL-verschlüsselt zwischen dem Web-Browser und dem iRMC übertragen.

LDAP SSL Enabled

Wenn Sie diese Option aktivieren, erfolgt der Datenaustausch zwischen iRMC und Directory Server SSL-verschlüsselt.

LDAP SSL Enable hat keinen Einfluss darauf, ob die Seiten der iRMC-Web-Oberfläche SSL-gesichert geöffnet werden oder nicht.

LDAP SSL Enable sollten Sie nur aktivieren, wenn ein Domain Controller-Zertifikat installiert ist.

Disable Local Login

Wenn Sie diese Option aktivieren, werden alle iRMC-lokalen Benutzerkennungen gesperrt, und nur die durch den Directory Service verwalteten Benutzkennungen sind gültig.

ACHTUNG!

Wenn die Option *Disable Local Login* aktiviert ist und außerdem die Verbindung zum Directory Service fehlschlägt, ist am iRMC kein Login mehr möglich.

Always use SSL Login

Diese Option ist nur relevant, wenn gleichzeitig LDAP deaktiviert ist.

Wenn Sie diese Option aktivieren, wird stets die HTTP SSL-gesicherte Login-Seite verwendet, auch wenn LDAP deaktiviert ist. Nur wenn Sie *Always use SSL Login* nicht aktivieren und außerdem LDAP deaktiviert ist, kommt eine über Digest Authentication Login gesicherte Maske zum Einsatz.

Directory Server Type

Typ des verwendeten Directory Servers:

Folgende Directory Services werden unterstützt:

- *Active Directory*: Microsoft Active Directory
- *Novell*: Novell eDirectory
- *OpenLDAP*: OpenLDAP

► Klicken Sie auf die Schaltfläche *Apply*, um Ihre Einstellungen zu aktivieren.

Je nach gewähltem Directory Service werden unterschiedliche Eingabefelder angeboten:

- Zu *Active Directory* siehe „iRMC für Microsoft Active Directory konfigurieren“ auf Seite 276.
- Zu *eDirectory* und *Open LDAP* siehe „iRMC für Novell eDirectory / OpenLDAP konfigurieren“ auf Seite 278.

iRMC für Microsoft Active Directory konfigurieren

Nachdem Sie Ihre Wahl *Active Directory* mit *Apply* bestätigt haben, wird die folgende Variante der Seite *Directory Service Configuration* angezeigt:

Bild 130: Global Directory Service Configuration: Angaben für Microsoft Active Directory

Die in Bild 130 beispielhaft dargestellten Eingaben beziehen sich auf die im Abschnitt „iRMC-Benutzerverwaltung via Microsoft Active Directory“ auf Seite 80 dargestellten Beispiele und Abbildungen.

Gehen Sie wie folgt vor:

- Vervollständigen Sie Ihre Angaben Sie in der Gruppe *Global Directory Service Configuation.*

  LDAP Server 1
  IP-Adresse oder DNS-Name des zu verwendenden LDAP Directory Servers.

  LDAP Server 2
  IP-Adresse oder DNS-Name des LDAP Directory Servers, der als Backup Server geführt und bei Ausfall von *LDAP Server 1* als Directory Server herangezogen wird.

  Domain name
  Vollständiger DNS-Pfadname des Directory Servers.

  Base DN
  Base DN wird automatisch von *Domain name* abgeleitet.

  Department name
  Abteilungsname. Der Abteilungsname wird im Directory Service zur Bestimmung der Benutzerrechte benötigt. Ein Benutzer kann für den Server der Abteilung X andere Rechte besitzen als für den Server der Abteilung Y (siehe auch Bild 17 auf Seite 73).

- Klicken Sie in der Gruppe *Global Directory Service Configuation* auf die Schaltfläche *Apply*, um Ihre Einstellungen in *Global Directory Service Configuation* zu aktivieren.

  Die Directory Service-Konfiguration ist damit abgeschlossen und aktiviert.

Die Angaben in der Gruppe *Directory Service Access Configuration* sind für Microsoft Active Directory derzeit nicht relevant.
Die hier vorzunehmenden Einstellungen werden für die Alarmbenachrichtigung (Alerting) im Zusammenhang mit globalen Benutzerkennungen benötigt. Alerting wird derzeit jedoch nur für lokale Benutzerkennungen unterstützt.

iRMC für Novell eDirectory / OpenLDAP konfigurieren

Nachdem Sie Ihre Wahl *Novell* oder *OpenLDAP* mit *Apply* bestätigt haben, wird die nachfolgend beschriebene Variante der Seite *Directory Service Configuration* angezeigt.

Der Aufbau der Seite *Directory Service Configuration* ist für Novell eDirectory und OpenLDAP identisch.

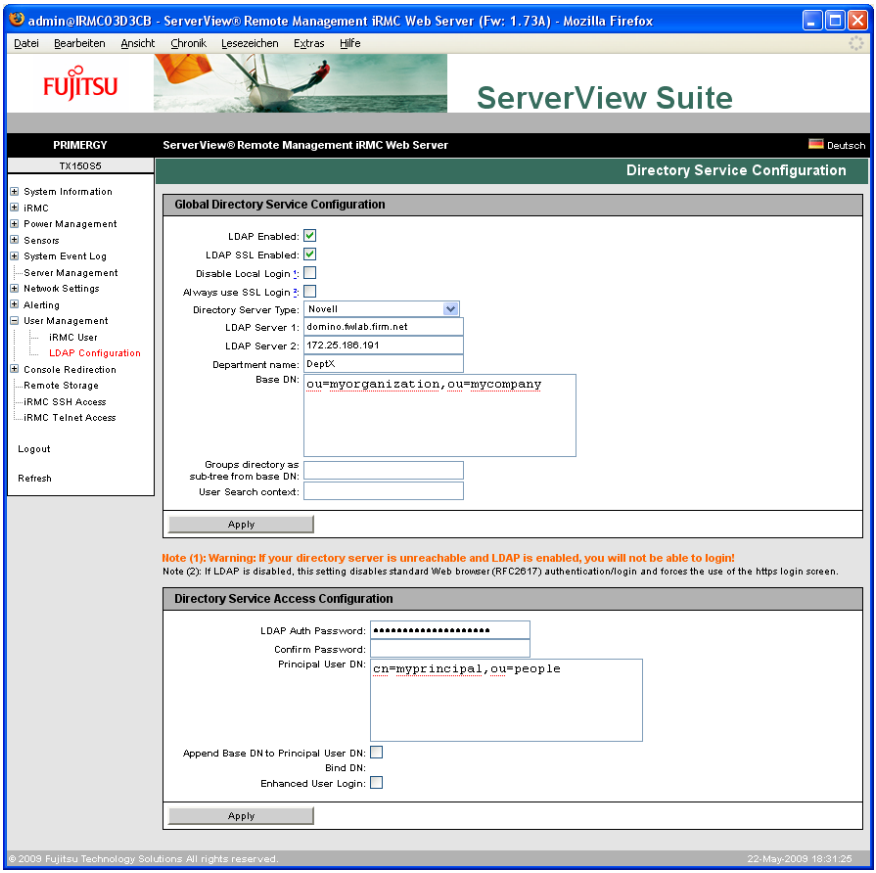


Bild 131: Global Directory Service Configuration: Angaben für Novell eDirectory / Open LDAP

Die in Bild 131 beispielhaft dargestellten Eingaben beziehen sich auf die im Abschnitt „iRMC-Benutzerverwaltung via Novell eDirectory“ auf Seite 98 dargestellten Beispiele und Abbildungen.

Gehen Sie wie folgt vor:

- Vervollständigen Sie Ihre Angaben Sie in der Gruppe *Global Directory Service Configuation.*

  LDAP Server 1
  IP-Adresse oder DNS-Name des zu verwendenden LDAP Directory Servers.

  LDAP Server 2
  IP-Adresse oder DNS-Name des LDAP Directory Servers, der als Backup Server geführt und bei Ausfall von *LDAP Server 1* als Directory Server herangezogen wird.

  Dept. name
  Abteilungsname. Der Abteilungsname wird im Directory Service zur Bestimmung der Benutzerrechte benötigt. Ein Benutzer kann für den Server der Abteilung X andere Rechte besitzen als für den Server der Abteilung Y (siehe auch Bild 17 auf Seite 73).

  Base DN
  Der *Base DN* ist der Full Distinguished Name des eDirectory bzw. Open LDAP Servers und repräsentiert den Baum oder Teilbaum, in dem die OU (Organizational Unit) *iRMCgroups* enthalten ist. Dieser DN bildet den Ausgangspunkt für LDAP-Suchoperationen.

  Group DN Context
  Pfadname der OU *iRMCgroups* als Teilbaum von *Base DN*.

  User Search DN
  Pfadname der OU *Users* als Teilbaum von *Base DN*.

- Klicken Sie in der Seite *Directory Service Configuation* auf die Schaltfläche *Apply*, um Ihre Einstellungen in *Global Directory Service Configuation* zu aktivieren.

- Tragen Sie in der Gruppe *Global Service Access Configuration* die folgenden Angaben ein:

  LDAP Auth Password
  Passwort, mit dem sich der Principal User beim LDAP-Server authentisiert.

  Confirm Password
  Wiederholen Sie das unter *LDAP Auth Password* eingegebene Passwort.

Principal User DN

Fully Distinguished Name der generischen iRMC-Benutzerkennung (Principal User), unter der der iRMC vom LDAP-Server die Benutzerberechtigungen der iRMC-Benutzer erfragt.

Append Base DN to Principal User DN

Wenn Sie diese Option aktivieren, brauchen Sie den Base DN unter *Principal User DN* nicht angeben. Es wird dann der Base DN verwendet, den Sie in der Gruppe *Global Directory Service Configuration* unter *Base DN* spezifiziert haben.

Bind DN

Unter *Bind DN* wird der Principal User DN angezeigt, wie er für die LDAP-Authentifizierung verwendet wird.

Enhanced User Login

Erhöhte Flexibilität beim Benutzer-Login.

Wenn Sie *Enhanced User Login* markieren und mit *Apply* aktivieren, wird ein zusätzliches Eingabefeld *User Login Search Filter* angezeigt, das mit dem Standard-Login-Suchfilter vorbelegt ist.

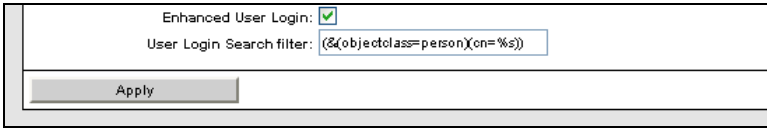


Bild 132: LDAP-Suchfilter für „Enhanced User Login“

Beim Login wird der Platzhalter „%s“ durch die jeweilige globale Benutzerkennung ersetzt. Den Standardfilter können Sie modifizieren, indem Sie z.B. anstatt „cn=“ ein anderes Attribut spezifizieren. Login-berechtigt am iRMC sind dann alle globalen Benutzkennungen, die den Bedingungen dieses Suchfilters genügen.

ACHTUNG!

Aktivieren Sie diese Option nur, wenn Sie mit der LDAP-Syntax vertraut sind. Wenn Sie versehentlich einen ungültigen Suchfilter spezifizieren und aktivieren, können sich Benutzer erst nach einer Deaktivierung der Option *Enhanced User Login* wieder unter einer globalen Benutzerkennung am iRMC einloggen.

► Klicken Sie auf die Schaltfläche *Apply*, um die Directory Service-Konfiguration abzuschließen und zu aktivieren.

7.13 Console Redirection - Konsolumleitung

Bei der Konsolumleitung können Sie zwischen folgenden Seiten wählen:

– „BIOS Text Console - Text-Konsolumleitung konfigurieren und starten“ auf Seite 281.
– „Advanced Video Redirection - Advanced Video Redirection (AVR) starten“ auf Seite 292.

7.13.1 BIOS Text Console - Text-Konsolumleitung konfigurieren und starten

Mithilfe der Seite *BIOS Text Console* können Sie die Text-Konsolumleitung konfigurieren und starten.

Die Text-Konsolumleitung kann auch im BIOS konfiguriert werden (siehe Abschnitt „Text-Konsolumleitung via LAN über das BIOS Setup konfigurieren“ auf Seite 44).

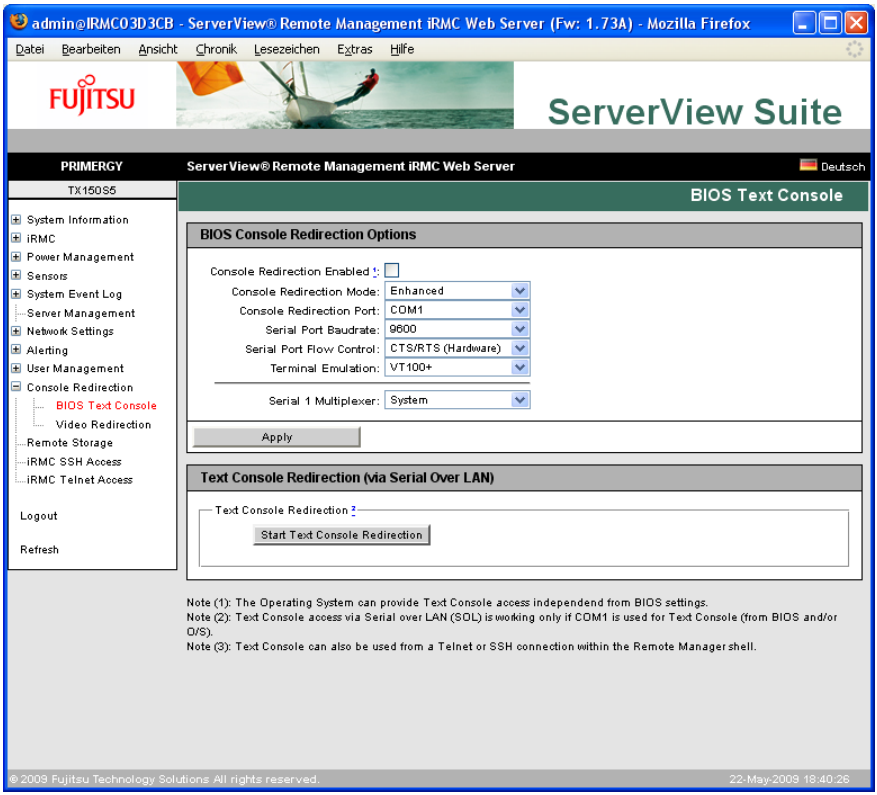

admin@IRMC03D3CB - ServerView® Remote Management iRMC Web Server (Fw: 1.73A) - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
FUJITSU
ServerView Suite
PRIMERGY
ServerView® Remote Management iRMC Web Server
Deutsch
TX150S5
System Information
iRMC
Power Management
Sensors
System Event Log
Server Management
Network Settings
Alerting
User Management
Console Redirection
BIOS Text Console
Video Redirection
Remote Storage
iRMC SSH Access
iRMC Telnet Access
Logout
Refresh
BIOS Text Console
BIOS Console Redirection Options
Console Redirection Enabled 1:
Console Redirection Mode: Enhanced
Console Redirection Port: COM1
Serial Port Baudrate: 9600
Serial Port Flow Control: CTS/RTS (Hardware)
Terminal Emulation: VT100+
Serial 1 Multiplexer: System
Apply
Text Console Redirection (via Serial Over LAN)
Text Console Redirection 2:
Start Text Console Redirection
Note (1): The Operating System can provide Text Console access independend from BIOS settings.
Note (2): Text Console access via Serial over LAN (SOL) is working only if COM1 is used for Text Console (from BIOS and/or O/S).
Note (3): Text Console can also be used from a Telnet or SSH connection within the Remote Manager shell.
© 2009 Fujitsu Technology Solutions All rights reserved.
22-May-2009 18:40:26

Bild 133: Seite BIOS Text Console

7.13.1.1 Bios Console Redirection Options - Text-Konsolumleitung konfigurieren

Unter *BIOS Console Redirection Options* können Sie die Text-Konsolumleitung konfigurieren.

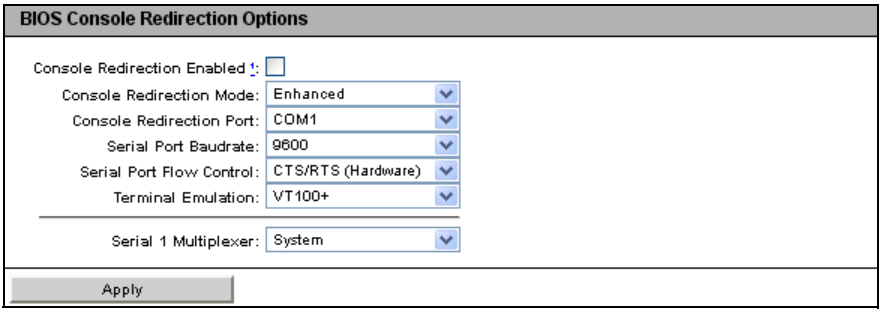


Bild 134: Seite BIOS Text Console - BIOS Console Redirection Options

Console Redirection Enabled

Mit dieser Option aktivieren/deaktivieren Sie die Konsolumleitung.

Das Betriebssystem kann die Text-Konsolumleitung auch unabhängig von den Einstellungen im BIOS ermöglichen.

Console Redirection Mode

Diese Einstellung wirkt sich auf das Verhalten der Konsolumleitung bei laufendem Betriebssystem (nach der BIOS POST-Phase) aus (siehe Abschnitt „Text-Konsolumleitung bei laufendem Betriebssystem“ auf Seite 290):

Standard

Die Konsolumleitung wird nach der POST-Phase des BIOS beendet.

Enhanced

Die Konsolumleitung steht über die POST-Phase des BIOS hinaus zur Verfügung.

Console Redirection Port

Es stehen zwei serielle Ports zur Verfügung: *Serial 1*, *Serial 2*.

Wenn die Konsolumleitung über LAN funktionieren soll, muss Serial 1 eingestellt sein.

Wenn *Serial 2* ausgewählt ist, funktioniert nur der Anschluss über Nullmodem-Kabel.

Serial Port Baud Rate

Folgende Baud Rates können eingestellt werden: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.

Serial Port Flow Control

Folgende Einstellungen sind möglich:

None

Die Flusskontrolle ist ausgeschaltet.

XON/XOFF (Software)

Die Flusskontrolle wird via Software durchgeführt.

CTS/RTS (Hardware)

Die Flusskontrolle wird via Hardware durchgeführt.

Terminal Emulation

Es werden folgende Terminal Emulationen angeboten:

VT100 7Bit, VT100 8Bit, *PC-ANSI 7Bit*, *PC-ANSI 8 Bit, VT100+*, *VT-UTF8*

Serial 1 Multiplexer

Prüfen Sie die Multiplexer-Einstellungen auf Konsistenz:

- Serial: System
- LAN: iRMC

► Klicken Sie auf die Schaltfläche *Apply,* um Ihre Einstellungen zu aktivieren.

7.13.1.2 Text Console Redirection (via Serial Over LAN) - Text-Konsolumleitung starten

Unter *Text Console Redirection (via Serial Over LAN)* können Sie die Text-Konsolumleitung starten.

Die Text-Konsolumleitung via Serial Over LAN (SOL) setzt voraus, dass Betriebssystem und/oder BIOS den seriellen Port 1 (COM1) für die Umleitung der Text-Konsole verwenden.

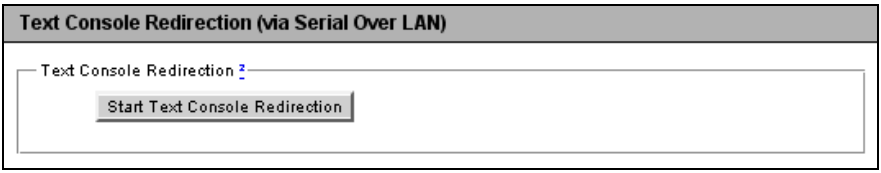


Bild 135: Text-Konsolumleitung via Serial Over LAN (SOL) starten

- Klicken Sie auf die Schaltfläche *Start Console Redirection*, um die Text-Konsolumleitung zu starten.

  Das JAVA-Applet für die Text-Konsolumleitung wird gestartet (siehe Bild 136 auf Seite 286):

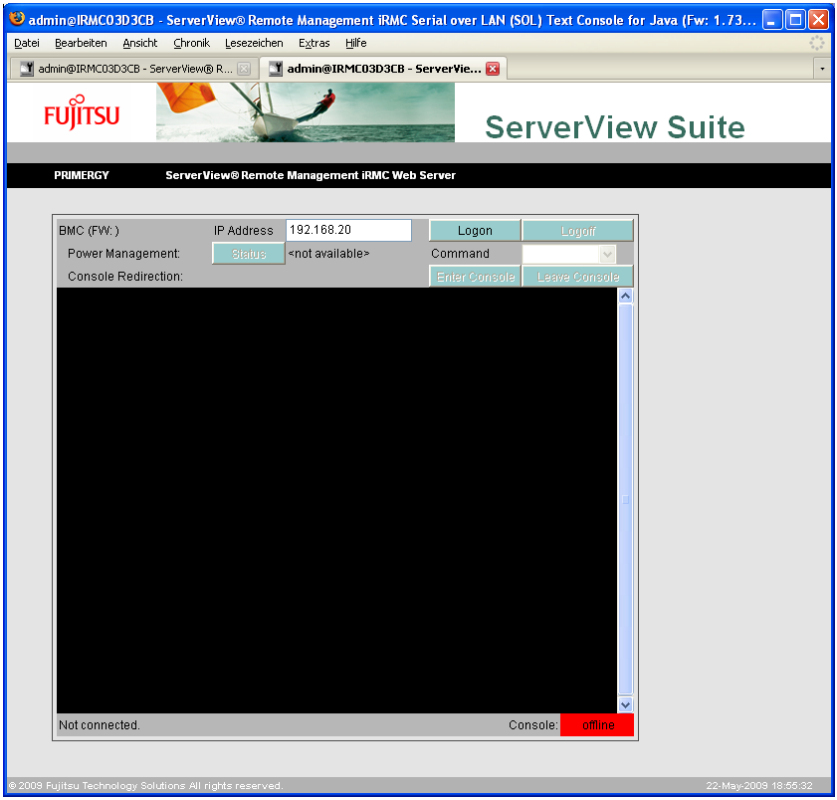


Bild 136: Fenster für Power Management und Text-Konsolumleitung (vor Login)

► Klicken Sie auf die Schaltfläche *Logon*, um sich am iRMC anzumelden.

Anschließend werden Sie zur Eingabe von iRMC-Benutzerkennung und -Passwort aufgefordert:

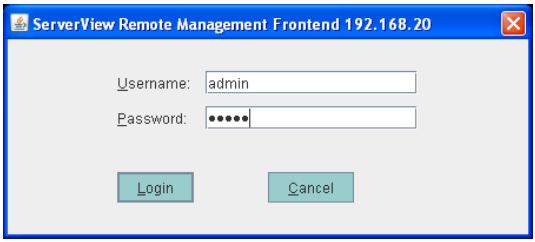


Bild 137: Power-Management und Text-Konsolumleitung - Login-Fenster

► Geben Sie Benutzerkennung und Passwort ein und bestätigen Sie durch Klicken auf *Login*.

Anschließend wird das Fenster für Power Management und Text-Konsolumleitung angezeigt:

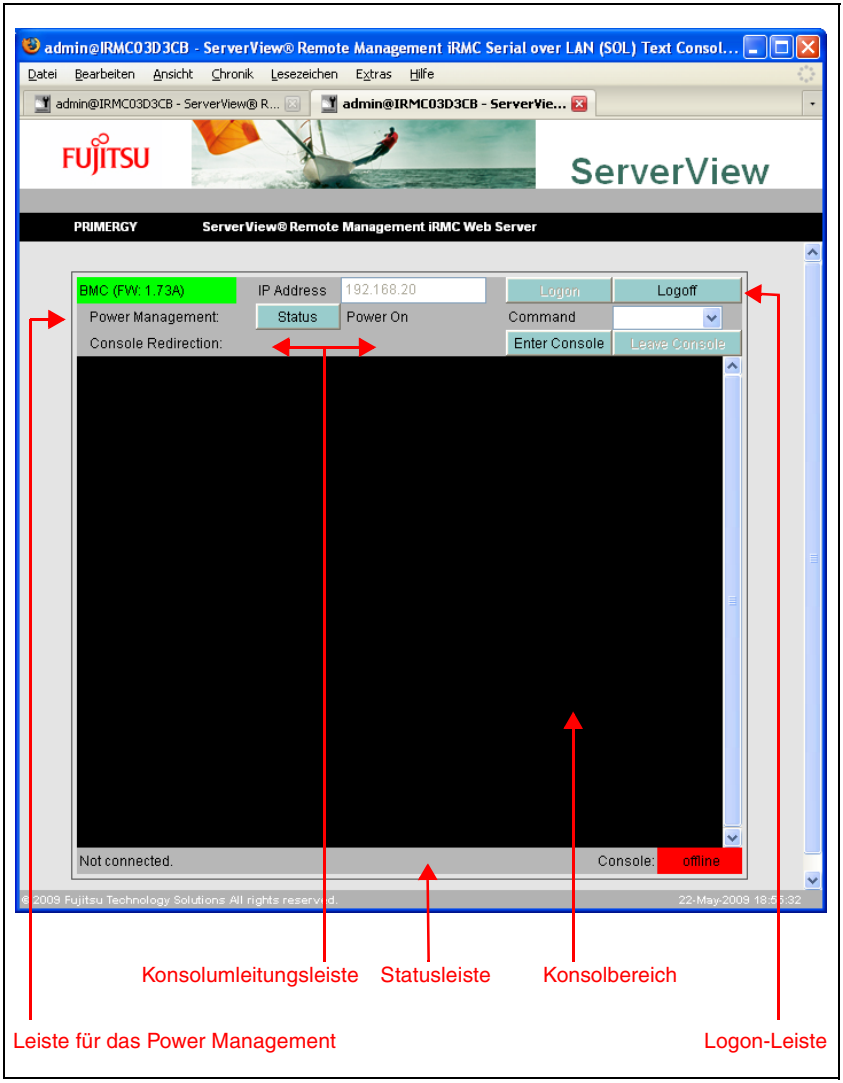


Bild 138: Fenster für Power Management und Text-Konsolumleitung

Nachfolgend sind die Elemente des Konsolumleitungsfensters erläutert:

Logon-Leiste
: In der Logon-Leiste werden IP-Adresse und aktuelle Firmware-Version des iRMC angezeigt. Über die Schaltflächen *Login* und *Logout* können Sie sich am iRMC einloggen bzw. ausloggen.

Leiste für das Power Management
: Die Leiste für das Power Management informiert über den Power Status des verwalteten Servers. Mithilfe der Schaltfläche *Status* können Sie die Anzeige aktualisieren.

  In der Dropdown-Liste *Command* können Sie ein IPMI-Kommando für das Power Management des verwalteten Servers auswählen und starten (siehe Seite Seite 289). Hierfür müssen Sie nicht mit der Konsoleverbunden sein.

Konsolumleitungsleiste
: In der Konsolumleitungsleiste können Sie mithilfe der Schaltflächen *Enter Console* und *Leave Console* die Anzeige im Konsolbereich ein- bzw. ausschalten.

Konsolbereich
: Der Konsolbereich enthält die Anzeigen der umgeleiteten Text-Konsole.

Statusleiste
: Die Statusleiste zeigt die IP-Adresse des iRMC sowie die Portnummer für die Konsolumleitung an. Außerdem informiert die Statusleiste über den Status der Konsolumleitung (online / offline).

► Klicken Sie auf *Enter Console*.

Danach sind Sie mit der Konsole verbunden und können das gewünschte Kommando ausführen, indem Sie es entweder direkt im Konsolbereich eingeben oder in der Dropdown-Liste *Command* (nur IPMI-Kommandos) anklicken:

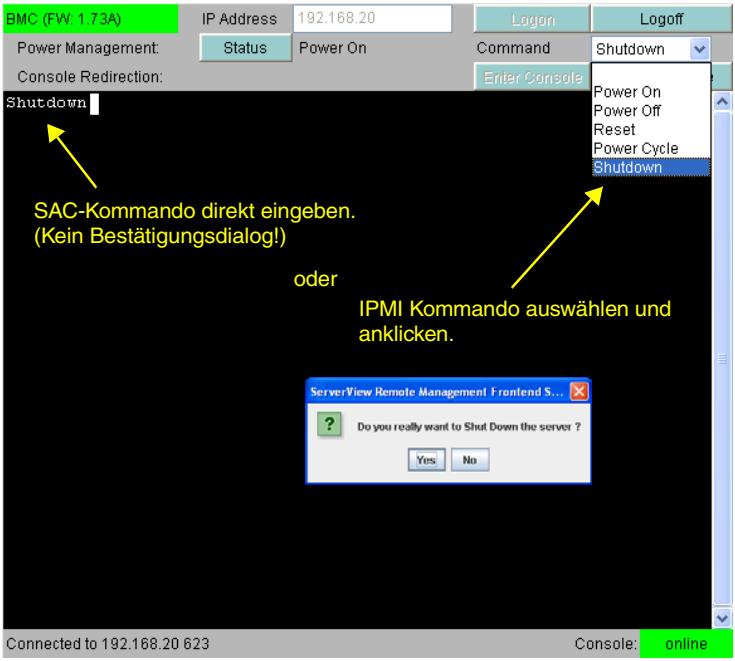


Bild 139: SAC- oder IPMI-Kommandos an der Text-Konsole eingeben.

IPMI-Kommando	Erläuterung
Power On	Schaltet den Server ein.
Power Off	Schaltet. den Server aus.
Reset	Startet den Server unabhängig vom Status des Betriebssystems komplett neu (Kaltstart).
Power Cycle	Schaltet den Server vollständig aus und nach ca. 5 Sekunden wieder ein.
Shutdown	Graceful Shutdown und Power Off.

► Um die Verbindung zur Konsole zu beenden, klicken Sie auf die Schaltfläche *Leave Console*.

7.13.1.3 Text-Konsolumleitung bei laufendem Betriebssystem

Sie können - je nach Betriebssystem des verwalteten Servers - auch nach der BIOS POST-Phase noch die Konsolumleitung nutzen.

DOS

Bedingung:

Die BIOS-Einstellung für den Modus der Konsolumleitung muss auf *Enhanced* konfiguriert sein (siehe Abschnitt „BIOS Text Console - Text-Konsolumleitung konfigurieren und starten“ auf Seite 281).

Wenn der verwaltete Server in Folge eines Problems die PRIMERGY ServerView Suite/Diagnose-Software startet, können Sie PRIMERGY ServerView Suite/Diagnose/Diagnose remote über eine Konsolumleitung bedienen.

Nähere Informationen zu PRIMERGY ServerView Suite/Diagnose finden Sie im Handbuch „RemoteView 5.0“.

Windows Server 2003

Windows Server 2003 übernimmt nach der POST-Phase automatisch die Konsolumleitung, ohne dass weitere Einstellungen notwendig sind. Während der Boot-Phase des Betriebssystems wird die SAC-Konsole von Windows Server 2003 übertragen:

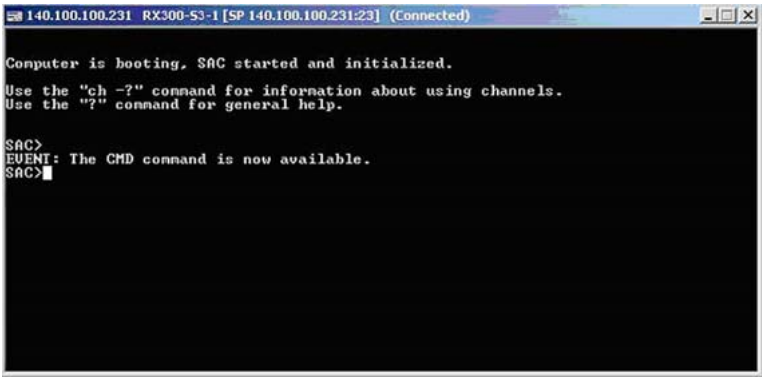

140.100.100.231 RX300-S3-1 [SP 140.100.100.231:23] (Connected)
Computer is booting, SAC started and initialized.
Use the "ch -?" command for information about using channels.
Use the "?" command for general help.
SAC>
EVENT: The CMD command is now available.
SAC>

Bild 140: SAC-Konsole von Windows Server 2003

Linux

Ein Linux-Betriebssystem müssen Sie konfigurieren, damit es die Konsolumleitung nach der POST-Phase übernimmt. Wenn es konfiguriert ist, haben Sie remote vollen Zugriff.

Notwendige Einstellungen

Die Einstellungen können sich je nach Programmversion etwas ändern.

SuSe und RedHat

Fügen Sie am Ende der Datei */etc/inittab* folgende Zeile an:

```
xx:12345:respawn:/sbin/agetty <baudrate> ttyS0
```

RedHat

Fügen Sie in die Datei */etc/grub.conf* folgenden Kernel-Boot-Parameter ein:

```
console=ttyS0,<baudrate> console=tty0
```

SuSE

Fügen Sie in die Datei */boot/grub/menu.lst* folgenden Kernel-Boot-Parameter ein:

```
console=ttyS0,<baudrate> console=tty0
```

7.13.2 Advanced Video Redirection - Advanced Video Redirection (AVR) starten

Mithilfe der Seite *Advanced Video Redirection* können Sie die grafische Konsolumleitung starten. Das Feature „Advanced Video Redirection“ leitet die grafische Ausgabe des verwalteten Servers zum Remote-Arbeitsplatz um und ordnet die Tastatur- und Mauseingaben des Remote-Arbeitsplatzes dem verwalteten Server zu, sodass Sie am Remote-Arbeitsplatz so auf den verwalteten Server zugreifen können, als bedienten Sie ihn vor Ort.

AVR kann von zwei Benutzern gleichzeitig verwendet werden. Dabei hat ein Benutzer die volle Kontrolle über den Server (Full Control-Modus), während der andere Benutzer die Bedienung des Servers via die Tastatur- und Mauseingaben nur passiv verfolgen kann (View Only-Modus).

Um die iRMC-Funktion *Advanced Video Redirection* nutzen zu können, benötigen Sie einen License Key (siehe „License Key auf den iRMC laden.“ auf Seite 196).

Die AVR-Funktionalität wird über ein Java Applet zur Verfügung gestellt.

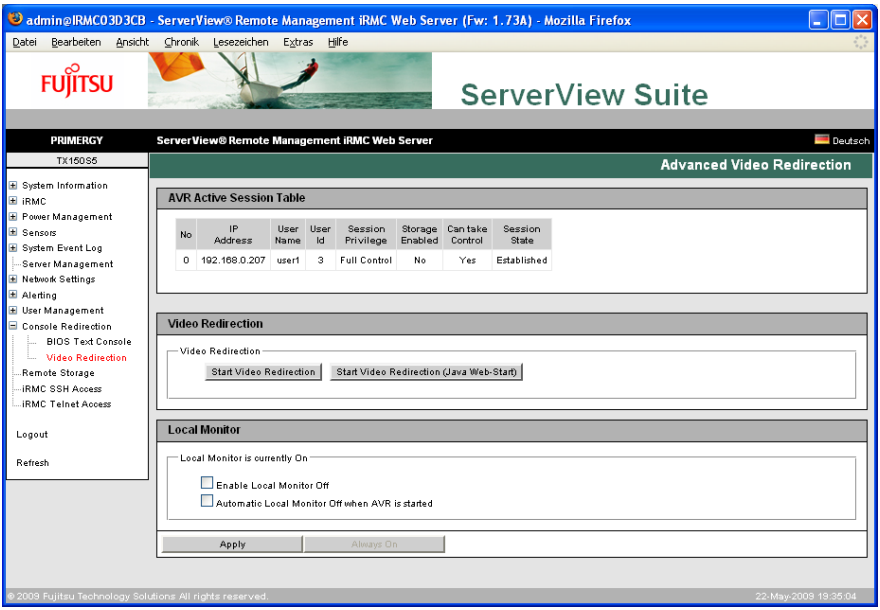


Bild 141: Seite Advanced Video Redirection

AVR Active Session Table - Anzeige der aktuellen AVR-Sitzungen

Unter *AVR Active Session Table* werden die zurzeit aktiven AVR-Sitzungen aufgelistet. Falls aktuell keine AVR-Sitzung aktiv ist, wird *AVR Active Session Table* nicht angezeigt.

Local Monitor - Ein-/Ausschalt-Optionen für den server-lokalen Monitor

Diese Funktion wird nicht von allen PRIMERGY-Servern mit iRMC unterstützt.

Unter *Local Monitor* wird der Status des lokalen Monitors am verwalteten Server angezeigt (siehe Abschnitt „Local Monitor Off-Funktionalität“ auf Seite 141).

Darüber hinaus können Sie konfigurieren,

– dass sich der lokale Monitor vom Remote-Arbeitsplatz aus ein- und ausschalten lässt,

– dass sich der lokale Monitor beim Start einer AVR-Sitzung automatisch für die Dauer der AVR-Sitzung ausschaltet.

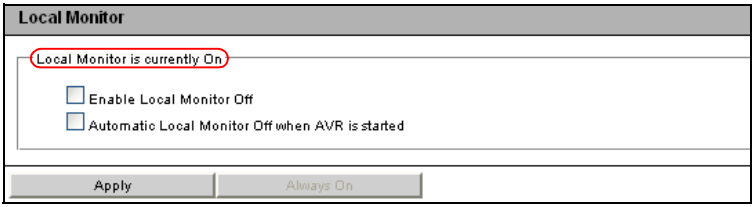


Bild 142: Seite Advanced Video Redirection - Local Monitor

Enable Local Monitor Off

Mit dieser Option aktivieren Sie die folgenden Möglichkeiten:

– Im Full Control-Modus einer AVR-Sitzung können Sie den lokalen Monitor aus- und einschalten (AVR-Menü *Extras*, siehe Seite 152).

– Für **Benutzer mit Administrator- oder OEM-Berechtigung** ist außerdem die alternierende Schaltfläche *Turn Off* / *Turn On* aktiviert, über die sich der lokale Monitor ebenfalls aus- und einschalten lässt (siehe Bild 143).

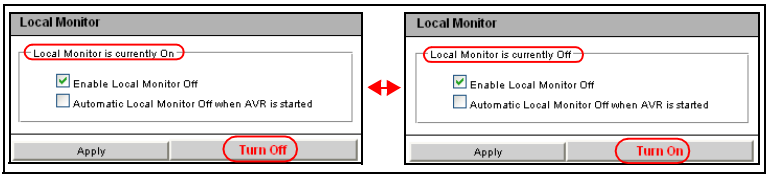


Bild 143: Seite Advanced Video Redirection - Local Monitor On/Off

– Zusätzlich können Sie konfigurieren, dass sich der lokale Monitor automatisch beim Start einer AVR-Sitzung für die Dauer dieser AVR-Sitzung ausschaltet (siehe Option *Automatical Local Monitor Off when AVR is started* auf Seite 295).

Sofern nicht eine parallele AVR-Sitzung mit Local Monitor Off aktiv ist, schaltet sich der lokale Monitor beim Beenden der AVR-Sitzung automatisch wieder ein.

Automatical Local Monitor Off when AVR is started

Diese Option ist nur wirksam, wenn *Enable Local Monitor* aktiviert ist.

Wenn Sie diese Option aktivieren, schaltet sich der lokale Monitor jeweils beim Start einer AVR-Sitzung automatisch für die Dauer dieser AVR-Sitzung aus. Nach Beenden der AVR-Sitzung schaltet sich der lokale Monitor automatisch wieder ein, sofern keine weitere AVR-Sitzung mit Local Monitor Off aktiv ist.

Parallele AVR-Sitzungen:

Auch wenn Sie während Ihrer AVR-Sitzung den lokalen Monitor einschalten (im AVR-Menü *Extras* oder über die Schaltfläche *Turn On*), schaltet sich der lokale Monitor beim Start einer neuen, parallelen AVR-Sitzung automatisch wieder aus.

Wenn alle AVR-Sitzungen beendet sind, schaltet sich der lokale Monitor automatisch wieder ein.

► Klicken Sie auf die Schaltfläche *Apply,* um Ihre Einstellungen zu aktivieren.

Video Redirection - AVR starten

Unter *Video Redirection* starten Sie die AVR.

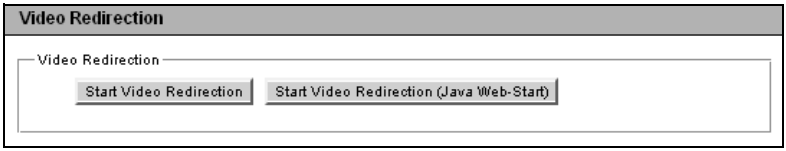


Bild 144: Seite Advanced Video Redirection - AVR starten

- Klicken Sie auf die Schaltfläche *Start Video Redirection* oder *Start Video Redirection (Java Web Start)* um eine (zweite) AVR-Sitzung zu starten.

  Das Java-Applet für die Advanced Video Redirection wird gestartet.

Das Java-Applet zeigt das AVR-Fenster im View Only-Modus an und Sie werden gefragt, ob Sie via AVR volle Kontrolle über den verwalteten Server erlangen wollen oder im View Only-Modus verbleiben wollen.

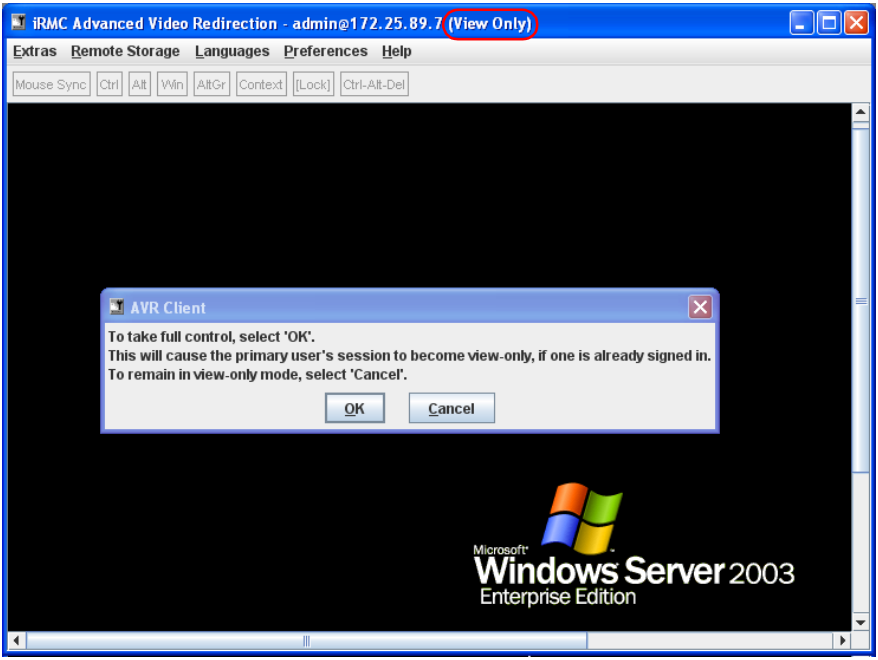

iRMC Advanced Video Redirection - admin@172.25.89.7 (View Only)
Extras Remote Storage Languages Preferences Help
Mouse Sync Ctrl Alt Win AltGr Context [Lock] Ctrl-Alt-Del
AVR Client
To take full control, select 'OK'.
This will cause the primary user's session to become view-only, if one is already signed in.
To remain in view-only mode, select 'Cancel'.
OK
Cancel
Microsoft
Windows Server 2003
Enterprise Edition

Bild 145: AVR-Fenster (View Only-Modus)

- Klicken Sie auf *OK*, wenn Sie volle Kontrolle über den verwalteten Server erlangen wollen. In diesem Fall wird das Fenster für die aktive Nutzung der AVR geöffnet (siehe Bild 146).

  Die zurzeit aktive AVR-Sitzung wird dadurch in den View Only-Modus versetzt. Die Benutzer sollten sich über den Modus ihrer Sitzungen absprechen.

- Klicken Sie auf *Cancel*, wenn Sie im View Only-Modus verbleiben wollen.

Falls Sie sich für die aktive Nutzung der AVR entschieden haben, wird das folgende Fenster angezeigt, über das Sie sich am verwalteten Server anmelden können.

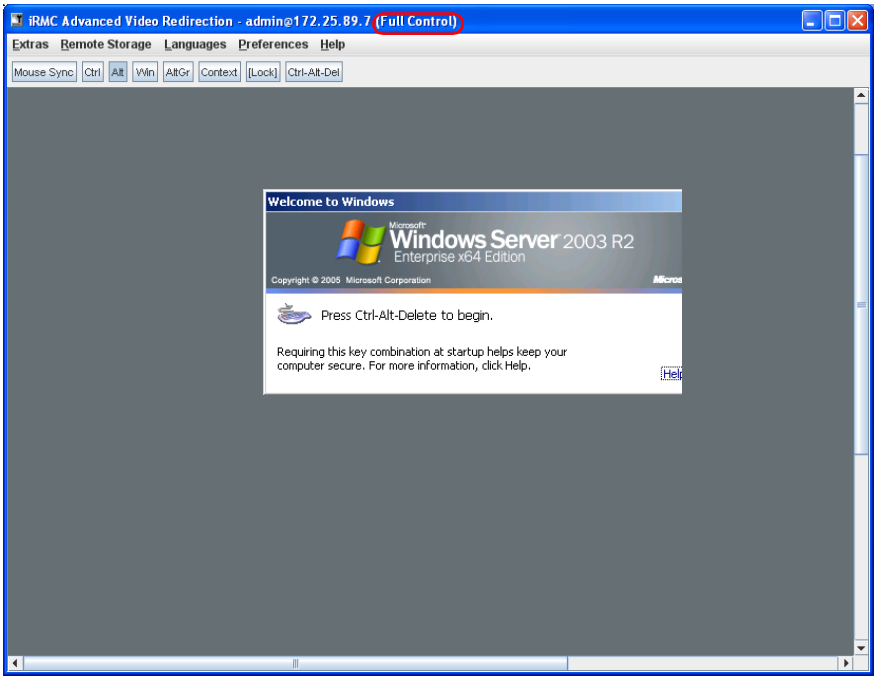

iRMC Advanced Video Redirection - admin@172.25.89.7 (Full Control)
Extras Remote Storage Languages Preferences Help
Mouse Sync Ctrl Alt Win AltGr Context [Lock] Ctrl-Alt-Del
Welcome to Windows
Windows Server 2003 R2
Enterprise x64 Edition
Copyright © 2005 Microsoft Corporation
Press Ctrl-Alt-Delete to begin.
Requiring this key combination at startup helps keep your computer secure. For more information, click Help.

Bild 146: AVR-Fenster (Full Control-Modus)

Die Menüs des AVR-Fensters sowie die integrierten Sondertasten sind im Kapitel „Advanced Video Redirection“ auf Seite 137 beschrieben.

Auf der Seite *Advanced Video Redirection* werden die beiden aktiven AVR-Sitzungen wie folgt angezeigt:

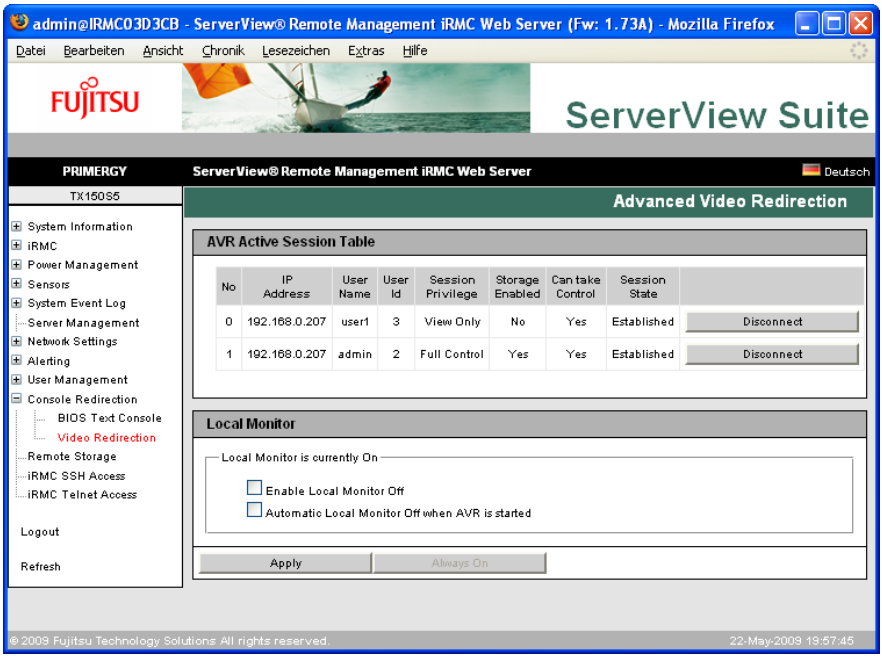


Bild 147: Seite Advanced Video Redirection bei zwei aktiven AVR-Sitzungen

Disconnect

Durch Klicken auf eine Schaltfläche *Disconnect* können Sie in einem Bestätigungsdialog die links neben dieser Schaltfläche angezeigte AVR-Sitzung beenden.

Mit *Disconnect* können Sie nur AVR-Sitzungen anderer Benutzer beenden. Um Ihre eigene Sitzung zu beenden, wählen Sie im AVR-Fenster: Menü *Extras* - *Exit* (siehe Seite 152).

Falls der verwaltete Server ausgeschaltet ist, wird das folgende Fenster angezeigt:

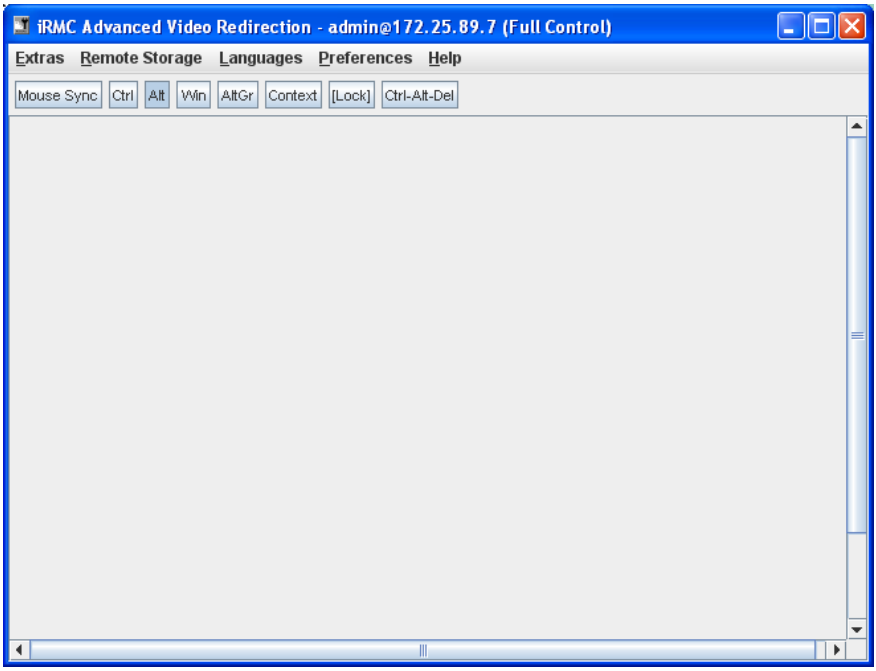


Bild 148: AVR-Fenster bei ausgeschaltetem Server

7.14 Remote Storage

Das Feature „Remote Storage“ stellt dem verwalteten Server ein „virtuelles“ Laufwerk zur Verfügung, das sich physisch an anderer Stelle im Netz befindet. Die Source für das virtuelle Laufwerk kann ein physisches Laufwerk (Disketten-Laufwerk, CD-ROM/DVD-ROM) oder ein ISO Image (Image-File) sein.

Um die iRMC-Funktion *Remote Storage* nutzen zu können, benötigen Sie einen gültigen License Key (siehe Seite 198).

Die Remote Storage-Speichermedien stellen Sie wahlweise wie folgt zur Verfügung:

– Am Remote Arbeitsplatz als physisches Laufwerk oder Image-File (siehe Seite 160). Das Image-File kann außerdem ein Netzlaufwerk sein (mit Laufwerksbuchstaben, z. B. „D:“ für Laufwerk D).

– Über einen Remote Storage Server zentral im Netz als Image-File (siehe Seite 169).

Parallele Remote Storage-Verbindungen:

Zur selben Zeit möglich sind entweder

– **maximal zwei** Remote Storage-Verbindungen zu virtuellen Laufwerken am Remote-Arbeitsplatz (bei Verbindungsaufbau via AVR Java-Applet)

oder

– **eine** Remote Storage-Verbindung zu einem Remote Storage Server.

Remote Storage-Verbindungen via Applet und Remote Storage Server sind nicht gleichzeitig möglich.

Mithilfe der Seite *Remote Storage* können Sie sich den Status der aktuellen Remote Storage-Verbindungen anzeigen lassen und außerdem die Verbindung zu einem Remote Storage Server herstellen.

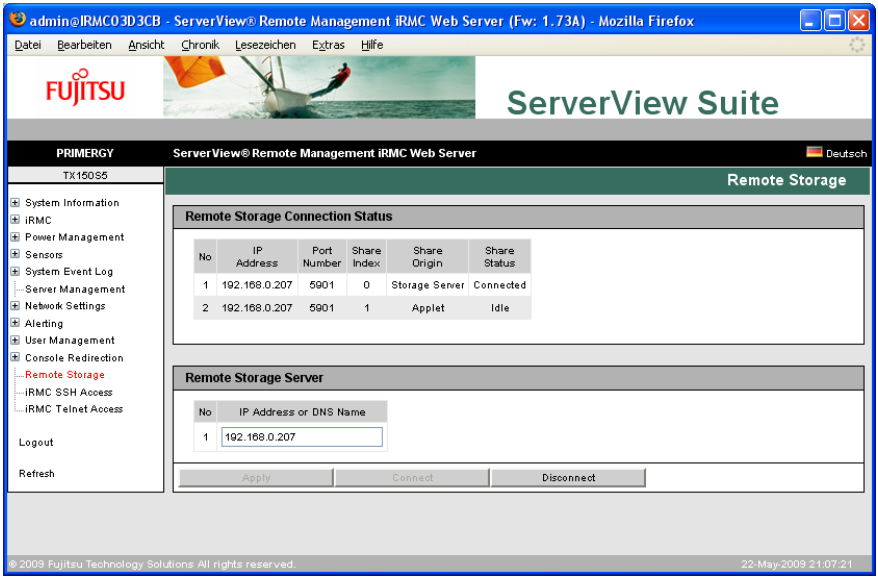


Bild 149: Seite Remote Storage

IP Address or DNS Name

Tragen Sie hier die IP-Adresse oder den DNS-Namen des Computers ein, auf dem ein Remote Storage Server installiert ist.

Apply

Wenn Sie auf die Schaltfläche *Apply* klicken, wird die IP-Adresse bzw. der DNS-Name des Remote Storage Servers gespeichert.

Connect

Wenn Sie auf die Schaltfläche *Apply* klicken, wird die IP-Adresse bzw. der DNS-Name des Remote Storage Servers gespeichert und die verbindung zum Remote Storage Server hergestellt.

Der Verbindungsaufbau zum Remote Storage Server setzt voraus, dass der Remote Storage Server installiert ist und zurzeit ausgeführt wird.

Disconnect

Durch Klicken auf die Schaltfläche *Disconnect* beenden Sie die Verbindung zum Remote Storage Server.

7.15 iRMC über Telnet / SSH (Remote Manager) bedienen

Für den iRMC gibt es eine Telnet/SSH-basierte Oberfläche - den so genannten Remote Manager. Die alphanumerische Bedienoberfläche des Remote Manager bietet Ihnen u.a. Zugriff auf System-und Sensorinformationen, das Power Management und den Error-Event-Log. Außerdem können Sie die Text-Konsolumleitung sowie eine SMASH CLP Shell starten.

Von der iRMC-Web-Oberfläche aus rufen Sie den Remote Manager wie folgt auf:

– Über den Link *iRMC SSH Access* initiieren Sie eine durch SSH (**S**ecure **Sh**ell) kryptographisch abgesicherte Telnet-Verbindung zum iRMC.

– Über den Link *iRMC Telnet Access* initiieren Sie eine nicht-gesicherte Telnet-Verbindung zum iRMC.

Maximale Anzahl paralleler Sitzungen:

– Telnet: maximal 4
– SSH: maximal 2
– Telnet und SSH insgesamt: maximal 4

Die Bedienung des iRMC über den Remote Manager ist beschrieben im Kapitel „iRMC über Telnet/SSH (Remote Manager) bedienen“ auf Seite 307.

Voraussetzung am verwalteten Server

Für den iRMC muss der Zugriff über Telnet aktiviert sein (siehe Abschnitt „Ports and Network Services - Ports und Netzdienste konfigurieren“ auf Seite 243).

Der Zugang über das Telnet-Protokoll ist aus Sicherheitsgründen standardmäßig deaktiviert, da Passwörter im Klartext übertragen werden.

SSH/Telnet-Verbindung aufbauen und beim Remote Manager einloggen

Wenn sich Bildschirm-Anzeigen für SSH- und Telnet-Verbindungen nur in den verbindungsspezifischen Anzeigen (Telnet oder SSH) unterscheiden, ist im Folgenden die Anzeige für eine SSH-Verbindung dargestellt.

► Klicken Sie in der Navigationsleiste auf den Link *iRMC SSH Access* (SSH) bzw. *iRMC Telnet Access* (Telnet).

Das Java-Applet für die SSH- bzw. Telnet-Verbindung wird gestartet und das folgende Fenster angezeigt (hier am Beispiel einer SSH-Verbindung):

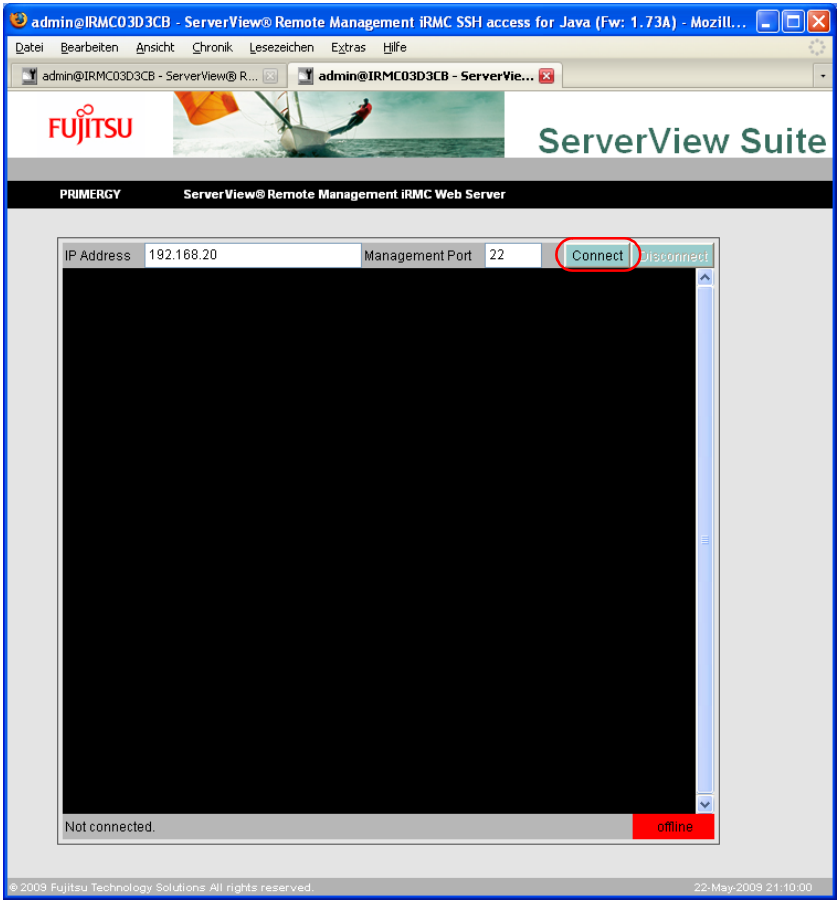


Bild 150: SSH-Verbindung zum iRMC aufbauen

► Klicken Sie in der Verbindungsleiste auf die Schaltfläche *Connect*.

Sobald die Verbindung zum iRMC aufgebaut ist, werden Sie zur Eingabe von Benutzerkennung und Passwort aufgefordert:

– *Einloggen beim Remote Manager über eine SSH-Verbindung*

Falls der Host-Key des verwalteten Servers noch nicht am Remote-Arbeitsplatz registriert ist, meldet der SSH-Client einen Security-Alert mit Vorschlägen für das weitere Vorgehen.

Es wird das folgende Anmeldefenster angezeigt:

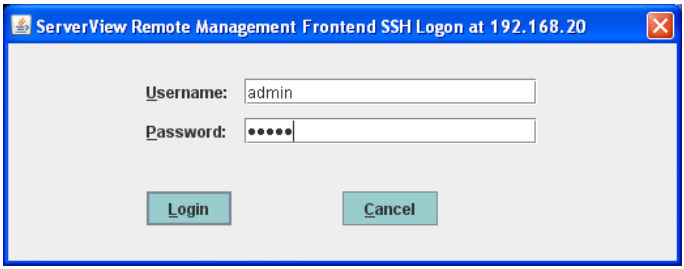


Bild 151: SSH-Verbindung: Anmelden beim Remote Manager

► Geben Sie Benutzerkennung und Passwort ein und bestätigen Sie Ihre Eingaben durch Klicken auf die Schaltfläche *Login*.

Anschließend wird das Hauptmenü des Remote Manager angezeigt (siehe Bild 153 auf Seite 306).

– *Einloggen beim Remote Manager über eine Telnet-Verbindung*

Es wird das Login-Fenster des Remote Manager angezeigt:

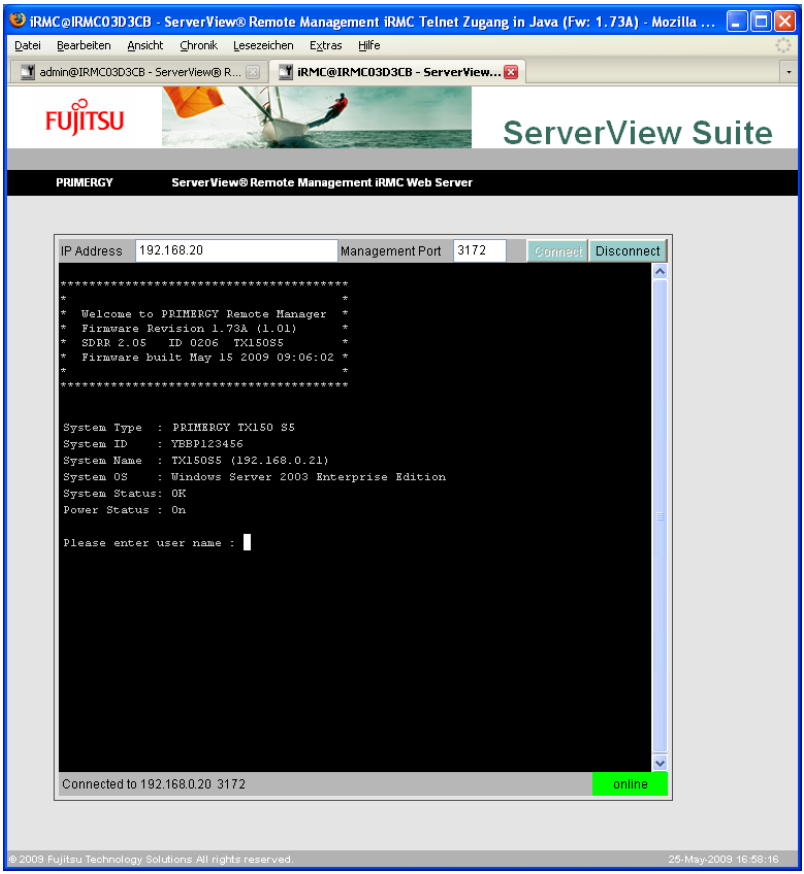

iRMC@IRMC03D3CB - ServerView® Remote Management iRMC Telnet Zugang in Java (Fw: 1.73A) - Mozilla ...
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
admin@IRMC03D3CB - ServerView® R...
iRMC@IRMC03D3CB - ServerView...
FUJITSU
ServerView Suite
PRIMERGY
ServerView® Remote Management iRMC Web Server
IP Address
192.168.20
Management Port
3172
Connect
Disconnect
Welcome to PRIMERGY Remote Manager
Firmware Revision 1.73A (1.01)
SDRR 2.05 ID 0206 TX150S5
Firmware built May 15 2009 09:06:02
System Type : PRIMERGY TX150 S5
System ID : YBBP123456
System Name : TX150S5 (192.168.0.21)
System OS : Windows Server 2003 Enterprise Edition
System Status: OK
Power Status : On
Please enter user name :
Connected to 192.168.0.20 3172
online
© 2009 Fujitsu Technology Solutions All rights reserved.
25-May-2009 16:58:16

Bild 152: Telnet-Verbindung: Anmelden beim Remote Manager

Je nachdem, ob ServerView-Agenten auf dem System schon einmal gestartet wurden, wird das Login-Fenster mit oder ohne Systeminformationen angezeigt (siehe Seite 312).

► Geben Sie Benutzerkennung und Passwort ein und bestätigen Sie Ihre Eingaben durch Drücken der Taste Enter.

Anschließend wird das Hauptmenü des Remote Manager angezeigt (siehe Bild 153).

admin@IRMC03D3CB - ServerView® Remote Management iRMC SSH access for Java (Fw: 1.73A) - Mozilla Fi...
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
admin@IRMC03D3CB - ServerView® R...
admin@IRMC03D3CB - ServerVie...
FUJITSU
ServerView Suite
PRIMERGY ServerView® Remote Management iRMC Web Server
IP Address 192.168.20
Management Port 22
Connect
Disconnect
Welcome to PRIMERGY Remote Manager
Firmware Revision 1.73A (1.01)
SDRR 2.05 ID 0206 TX15085
Firmware built May 15 2009 09:06:02
System Type : PRIMERGY TX150 S5
System ID : YK4J008860
System Name : TX15085 (192.168.0.21)
System OS : Windows Server 2003 R2 Enterprise Edition
System Status: OK
Power Status : Off
Main Menu
(1) System Information...
(2) Power Management...
(3) Enclosure Information...
(4) Service Processor...
(c) Change password
(*) Console Redirection (EMS/SAC)
(s) Start a Command Line shell...
Enter selection or (0) to quit:
Connected to 192.168.20 ssh
online (SSH)
© 2009 Fujitsu Technology Solutions All rights reserved.
22-May-2009 21:10:00
Bild 153: Hauptmenü des Remote Manager

Telnet /SSH-Verbindung beenden

- Die Verbindung zum Remote Manager beenden Sie durch Klicken auf die Schaltfläche *Disconnect* in der Verbindungsleiste des Remote Manager-Fensters oder indem Sie im Hauptmenü des Remote Manager auf die Taste 0 drücken (siehe Bild 153).

8 iRMC über Telnet/SSH (Remote Manager) bedienen

Für den iRMC gibt es eine Telnet-basierte Oberfläche - den so genannten Remote Manager. Den Remote Manager können Sie über folgende Schnittstellen aufrufen:

– iRMC-Web-Oberfläche (siehe Seite 302)
– beliebiger Telnet/SSH-Client
– ServerView Remote Management Frontend

Der iRMC unterstützt gesicherte Verbindungen über SSH (**S**ecure **Sh**ell). Die Oberfläche des Remote Manager ist für Telnet und SSH-Verbindungen identisch. Im Prinzip kann jeder Telnet/SSH-Client, der VT100-Sequenzen versteht, für den Zugriff auf den iRMC verwendet werden. Es wird jedoch empfohlen, die iRMC-Web-Oberfläche oder das ServerView Remote Management Frontend (im Folgenden kurz: Remote Management Frontend) zu verwenden.

Maximale Anzahl paralleler Sitzungen:

– Telnet: maximal 4
– SSH: maximal 2
– Telnet und SSH insgesamt: maximal 4

Voraussetzung am verwalteten Server

Für den iRMC muss der Zugriff über Telnet aktiviert sein (siehe Abschnitt „Ports and Network Services - Ports und Netzdienste konfigurieren“ auf Seite 243).

Der Zugang über das Telnet-Protokoll ist aus Sicherheitsgründen standardmäßig deaktiviert, da Passwörter im Klartext übertragen werden.

Da ServerView den Wert des Management-Ports nicht kennt, arbeitet das Remote Management Frontend mit dem Default-Wert.

Da nach dem Start des Remote Management Frontends nicht automatisch eine Verbindung aufgebaut wird, können Sie einen vom Default-Wert abweichenden Wert für den Management-Port auch noch nach dem Start des Remote Management Frontends korrigieren.

8.1 iRMC über das ServerView Remote Management Frontend bedienen

Ausführliche Informationen zum Verbindungsaufbau zum iRMC über das Remote Management Frontend sowie zur Arbeitsumgebung des Remote Management Frontend finden Sie im Handbuch „ServerView Remote Management Frontend“.

8.2 Remote Manager

Im diesem Abschnitt sind Bedienung und Funktionen des iRMC über den Remote Manager im Einzelnen beschrieben. Am Ende des Abschnitts finden Sie außerdem einen kurzen Überblick über SMASH CLP.

8.2.1 Remote Manager bedienen

Anhand von Bild 154, das einen Ausschnitt aus dem Hauptmenü des Remote Manager zeigt, ist nachfolgend die Bedienung des Remote Manager exemplarisch dargestellt.

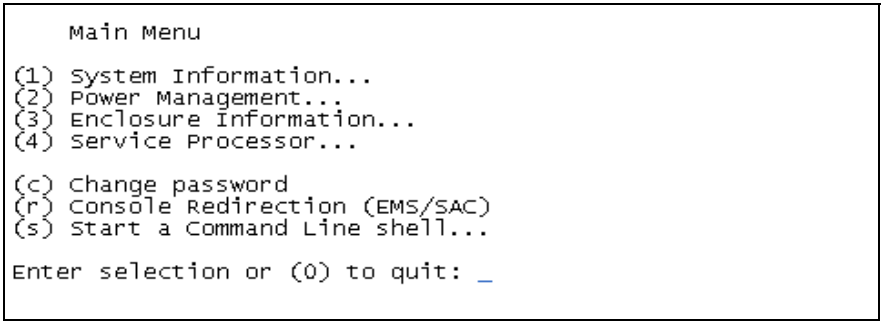


Bild 154: Bedienung des Remote Manager

- Den gewünschten Menüpunkt wählen Sie aus, indem Sie die Ziffer / den Buchstaben eingeben, der diesem Menüpunkt vorangestellt ist (z.B. „c“ für Change password).

  Funktionen, die einem Benutzer nicht erlaubt sind, sind mit einem Gedankenstrich (-) gekennzeichnet, Funktionen, die nicht verfügbar sind, mit einem Stern (*).

- Mit der Taste 0 oder der Tastenkombination Ctrl D beenden Sie den Remote Manager. Es wird ein entsprechendes Ereignis in das Event Log geschrieben.

8.2.2 Menü-Übersicht

Das Remote Manager Menü für den iRMC ist wie folgt strukturiert:

- **System Information**
  - Chassis Information
  - Mainboard Information
  - OS and SNMP Information
- **Power Management**
  - Immediate Power Off
  - Immediate Reset
  - Power Cycle
  - Power on
  - Graceful Power off (Shutdown)
  - Graceful Reset (Reboot)
- **Enclosure Information**
  - System Event-Log
    - View System Event-Log (text, newest first)
    - View System Event-Log (text, oldest first)
    - Dump System Event-Log (raw, newest first)
    - Dump System Event-Log (raw, oldest first)
    - View System Eventlog Information
    - Clear System Event-Log
  - Temperature
  - Voltages/Current
  - Fans
  - Power Supplies
  - Door Lock
  - CPU Sensors

  - Component Status (Lightpath)
  - List All Sensors
- **Service Processor**
  - Configure IP Parameters
  - List IP Parameters
  - Toggle Identify LED
  - Reset iRMC (Warm reset)
  - Reset iRMC (Cold reset)
- **Change password**
- **Console Redirection (EMS/SAC)**
- **Start a Command Line shell**

8.2.3 Anmeldeprozess

Sobald eine Verbindung zum iRMC aufgebaut ist, wird im Terminal Client am Remote-Arbeitsplatz das Login-Fenster des Remote Manager (Telnet/SSH-Fenster) angezeigt.

Je nachdem, ob ServerView-Agenten auf dem System schon einmal gestartet wurden, wird das Login-Fenster mit oder ohne Systeminformationen angezeigt.

Beim Anmelden über eine SSH-Verbindung: Falls der Host-Key des verwalteten Servers noch nicht am Remote-Arbeitsplatz registriert ist, meldet der SSH-Client einen Security-Alert mit Vorschlägen für das weitere Vorgehen.

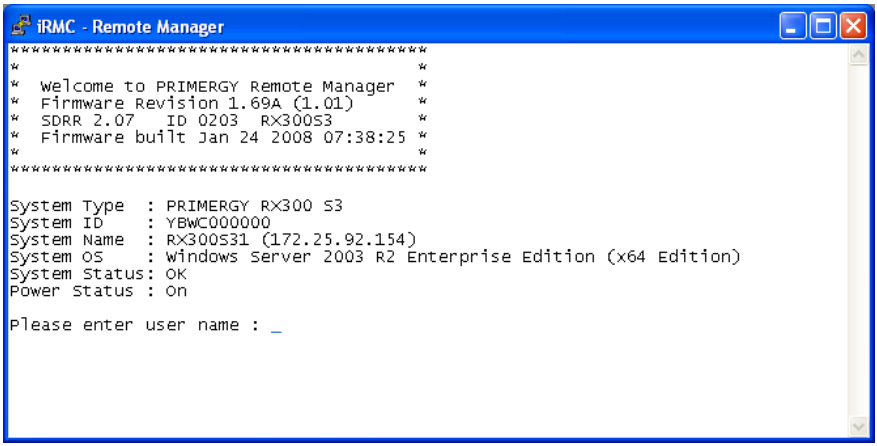

iRMC - Remote Manager
Welcome to PRIMERGY Remote Manager
Firmware Revision 1.69A (1.01)
SDRR 2.07 ID 0203 RX300S3
Firmware built Jan 24 2008 07:38:25
System Type : PRIMERGY RX300 S3
System ID : YBWC000000
System Name : RX300S31 (172.25.92.154)
System OS : Windows Server 2003 R2 Enterprise Edition (x64 Edition)
System Status: OK
Power Status : On
Please enter user name : _

Bild 155: Remote Manager: Login-Fenster (mit Systeminformation)

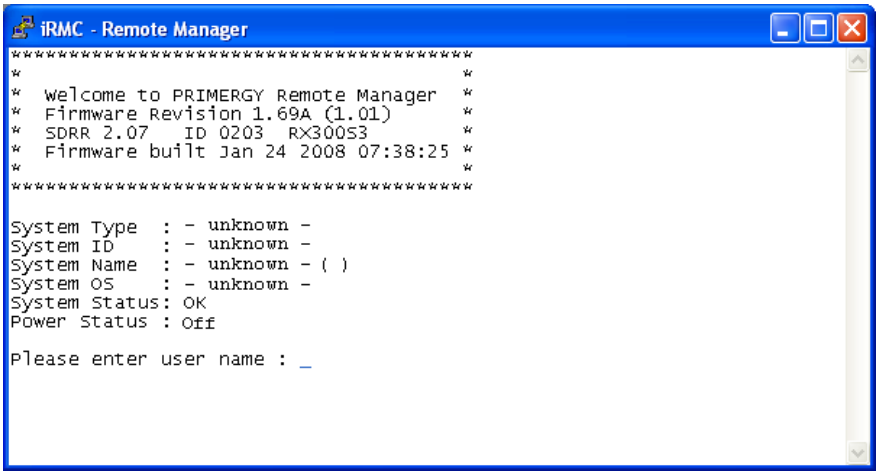

iRMC - Remote Manager
****
*   *
* Welcome to PRIMERGY Remote Manager   *
* Firmware Revision 1.69A (1.01)   *
* SDRR 2.07   ID 0203 RX300S3   *
* Firmware built Jan 24 2008 07:38:25 *
*   *
****
System Type : - unknown -
System ID   : - unknown -
System Name : - unknown - ( )
System OS   : - unknown -
System Status: OK
Power Status : Off
Please enter user name : _

Bild 156: Remote Manager: Login-Fenster (ohne Systeminformation)

Im Remote Manager-Fenster erhalten Sie Informationen zu dem betreffenden PRIMERGY System, anhand derer es sich identifizieren lässt, und zum Betriebszustand des Systems (Power Status). Einige Angaben (z. B. der System Name) werden nur für Server angezeigt und nur dann, wenn der Server entsprechend konfiguriert ist.

- Um den Remote Manager zu nutzen, müssen Sie sich mit einer Benutzerkennung und einem Passwort anmelden.

  Anschließend wird ein entsprechendes Ereignis in das Event-Log geschrieben und das entsprechende Hauptmenü des Remote Managers angezeigt (siehe Abschnitt „Hauptmenü des Remote Manager“ auf Seite 314).

  Sie können den Anmeldevorgang vorzeitig mit Ctrl D beenden.

8.2.4 Hauptmenü des Remote Manager

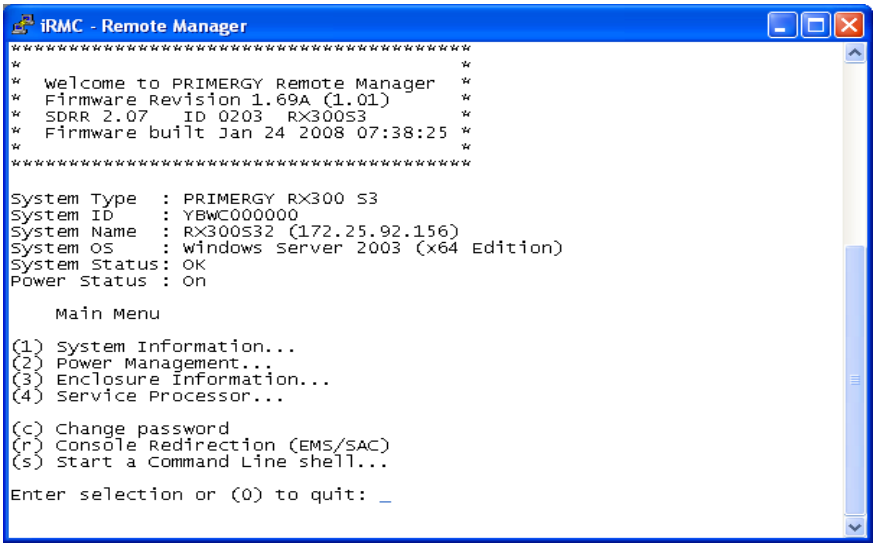

iRMC - Remote Manager
*****
* Welcome to PRIMERGY Remote Manager *
* Firmware Revision 1.69A (1.01) *
* SDRR 2.07 ID 0203 RX300S3 *
* Firmware built Jan 24 2008 07:38:25 *
*****
System Type : PRIMERGY RX300 S3
System ID : YBWC000000
System Name : RX300S32 (172.25.92.156)
System OS : Windows Server 2003 (x64 Edition)
System Status: OK
Power Status : On
Main Menu
(1) System Information...
(2) Power Management...
(3) Enclosure Information...
(4) Service Processor...
(c) Change password
(r) Console Redirection (EMS/SAC)
(s) Start a Command Line shell...
Enter selection or (0) to quit: _

Bild 157: Remote Manager: Hauptmenü-Fenster

Das Hauptmenü des Remote Managers bietet Ihnen folgende Funktionen:

System Information...	Informationen zum verwalteten Server einsehen (siehe Abschnitt „System Information - Informationen zum verwalteten Server“ auf Seite 318).
Power Management...	Server ein/ausschalten (siehe Abschnitt „Power Management“ auf Seite 319).
Enclosure Information...	Informationen über den aktuellen Systemzustand anfordern, z. B. Fehler- und Ereignismeldungen von Error-Log und Event-Log überprüfen (Temperatur, Lüfter, ...) (siehe Abschnitt „Enclosure Information - System Event-Log und Status der Sensoren“ auf Seite 321).
Service Processor...	Den iRMC konfigurieren (z. B. Firmware aktualisieren oder IP-Adresse ändern) (siehe Abschnitt „Service Processor - IP-Parameter, Identifizierungs-LED und Reset des iRMC“ auf Seite 325).
Change password	Passwort ändern (siehe Abschnitt „Passwort ändern“ auf Seite 317).
Console Redirection (EMS/SAC)	Text-Konsolumleitung (siehe Abschnitt „Console Redirection (EMS/SAC) - Text-Konsolumleitung starten“ auf Seite 326)
Start a Command Line shell...	Command Line Shell starten (siehe Abschnitt „Start a Command Line shell... - SMASH CLP Shell starten“ auf Seite 327)

Tabelle 8: Hauptmenü des Remote Managers

8.2.5 Erforderliche Benutzerberechtigungen

Tabelle 9 gibt einen Überblick, welche Benutzerberechtigungen zur Nutzung der einzelnen Funktionen des Remote Manager erforderlich sind.

Menüpunkte des Remote Manager	**Zulässig mit IPMI Privilege Level**				**Erforderliche Berechtigung**			
	OEM	**Administrator**	**Operator**	**User**	**Configure User Accounts**	**Configure iRMC Settings**	**Video Redirection Enabled**	**Remote Storage Enabled**
System Information...	X	X	X	X				
Power Management...	X	X	X					
Enclosure Information	X	X	X	X				
System Eventlog - View/Dump System Eventlog	X	X	X	X				
System Eventlog - Clear System Eventlog	X	X	X					
Sensor-Übersichten (*Temperature, Fans ...*)	X	X	X	X				
Service Processor...	X	X	X	X				
Service Processor... - Toggle Identify LED	X	X	X	X				
Service Processor... - List/Configure IP Parameters						X		
Service Processor... - Reset iRMC (warm/cold reset)	X	X						
Change Password					X			
Console Redirection (EMS/SAC)	X	X	X					
Start a command Line shell...	X	X	X	X				

Tabelle 9: Berechtigungen zur Nutzung des Remote Manager-Menüs

8.2.6 Passwort ändern

Mit dem Menüpunkt *Change password* kann ein Benutzer mit der Berechtigung *Configure User Accounts* (siehe Seite 62) sein eigenes Passwort sowie die Passwörter anderer Benutzer ändern.

8.2.7 System Information - Informationen zum verwalteten Server

Wenn Sie im Hauptmenü den Menüpunkt *System Information...* auswählen, erhalten Sie das folgende Menü:

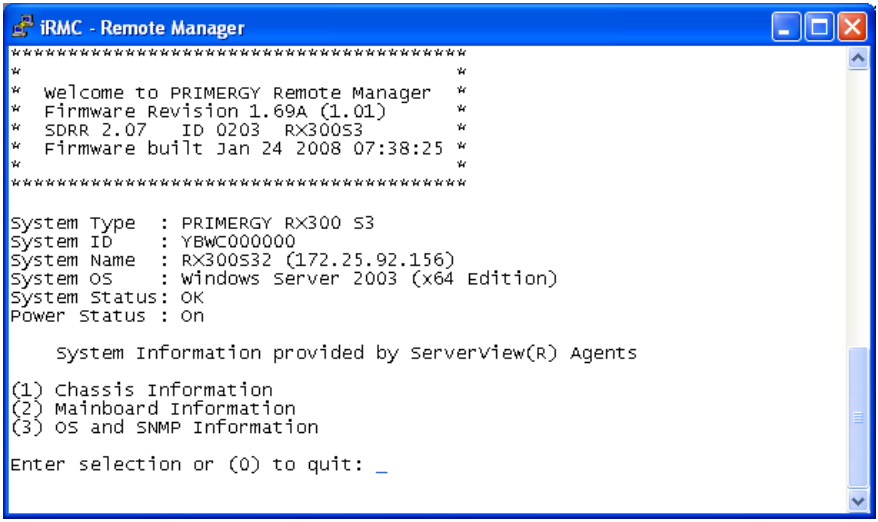

iRMC - Remote Manager
****
* Welcome to PRIMERGY Remote Manager *
* Firmware Revision 1.69A (1.01) *
* SDRR 2.07 ID 0203 RX300S3 *
* Firmware built Jan 24 2008 07:38:25 *
****
System Type : PRIMERGY RX300 S3
System ID : YBWC000000
System Name : RX300S32 (172.25.92.156)
System OS : Windows Server 2003 (x64 Edition)
System Status: OK
Power Status : On
System Information provided by ServerView(R) Agents
(1) Chassis Information
(2) Mainboard Information
(3) OS and SNMP Information
Enter selection or (0) to quit: _

Bild 158: Remote Manager: System Information-Fenster

Das Untermenü bietet Ihnen folgende Funktionen:

Chassis Information	Informationen über das Gehäuse des verwalteten Servers und seine Produktdaten.
Mainboard Information	Informationen zur Systembaugruppe des verwalteten Servers und ihren Produktdaten.
OS and SNMP Information	Informationen zum Betriebssystem und zur ServerView-Version des verwalteten Servers und zu den SNMP-Einstellungen.

Tabelle 10: Menü System Information

8.2.8 Power Management

Wenn Sie im Hauptmenü den Menüpunkt *Power Management...* auswählen, erhalten Sie das folgende Menü:

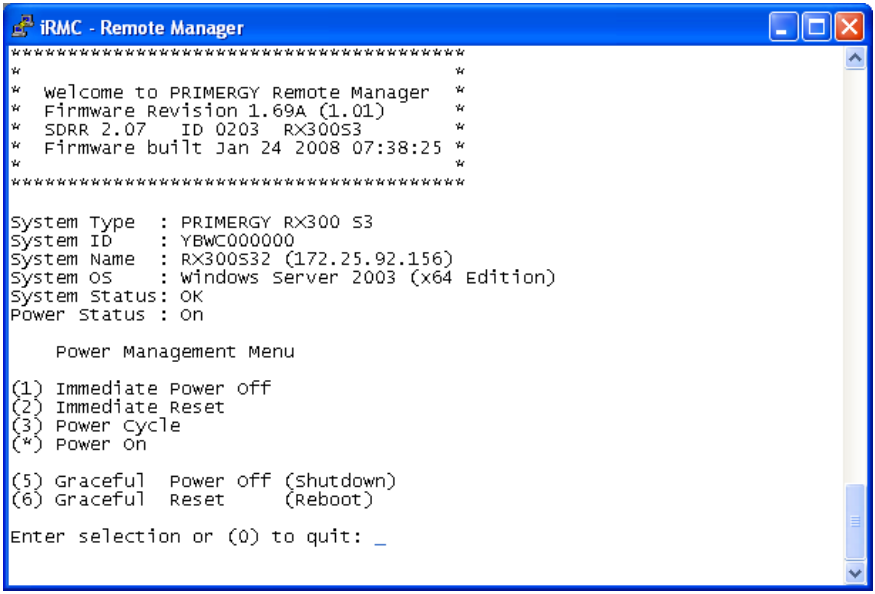

iRMC - Remote Manager
****
* Welcome to PRIMERGY Remote Manager *
* Firmware Revision 1.69A (1.01) *
* SDRR 2.07 ID 0203 RX300S3 *
* Firmware built Jan 24 2008 07:38:25 *
****
System Type : PRIMERGY RX300 S3
System ID : YBWC000000
System Name : RX300S32 (172.25.92.156)
System OS : Windows Server 2003 (x64 Edition)
System Status: OK
Power Status : On
Power Management Menu
(1) Immediate Power Off
(2) Immediate Reset
(3) Power Cycle
(*) Power On
(5) Graceful Power Off (Shutdown)
(6) Graceful Reset (Reboot)
Enter selection or (0) to quit: _

Bild 159: Remote Manager: Power Management-Fenster

Das Untermenü bietet Ihnen folgende Funktionen:

Immediate Power Off	Schaltet den Server unabhängig vom Status des Betriebssystems aus.
Immediate Reset	Startet den Server unabhängig vom Status des Betriebssystems komplett neu (Kaltstart).
Power Cycle	Schaltet den Server vollständig aus und nach einer konfigurierten Zeit automatisch wieder ein.
Power On	Schaltet den Server ein.
Graceful Power Off (Shutdown)	Graceful Shutdown und Power Off. Der Menüpunkt ist nur verfügbar, wenn ServerView-Agenten installiert und beim iRMC als „connected“ gemeldet sind.
Graceful Reset (Reboot)	Graceful Shutdown und Reboot. Der Menüpunkt ist nur verfügbar, wenn ServerView-Agenten installiert und beim iRMC als „connected“ gemeldet sind.

Tabelle 11: Menü Power Management

8.2.9 Enclosure Information - System Event-Log und Status der Sensoren

Wenn Sie im Hauptmenü den Menüpunkt *Enclosure Information...* auswählen, erhalten Sie das folgende Menü:

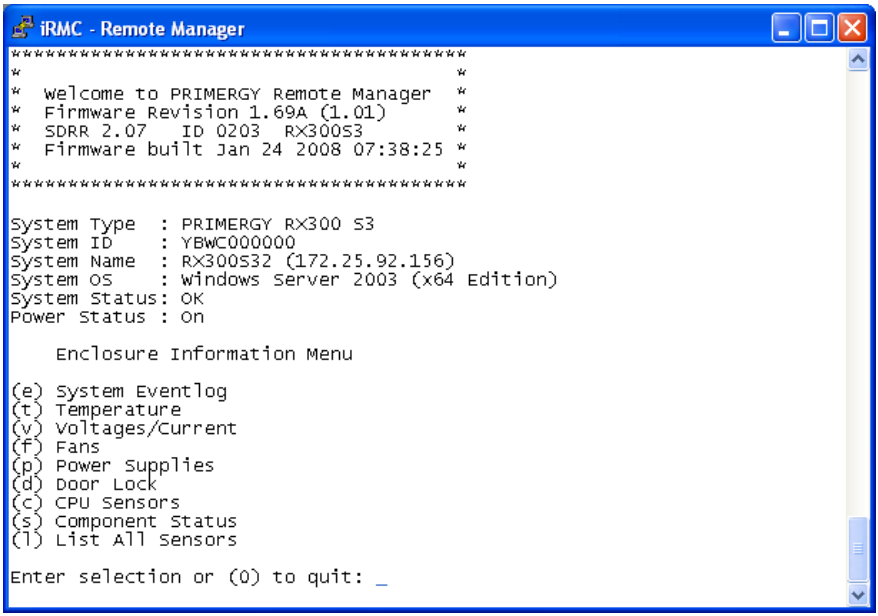

iRMC - Remote Manager
****
* Welcome to PRIMERGY Remote Manager *
* Firmware Revision 1.69A (1.01) *
* SDRR 2.07 ID 0203 RX300S3 *
* Firmware built Jan 24 2008 07:38:25 *
****
System Type : PRIMERGY RX300 S3
System ID : YBWC000000
System Name : RX300S32 (172.25.92.156)
System OS : Windows Server 2003 (x64 Edition)
System Status: OK
Power Status : On
Enclosure Information Menu
(e) System Eventlog
(t) Temperature
(v) Voltages/Current
(f) Fans
(p) Power Supplies
(d) Door Lock
(c) CPU Sensors
(s) Component Status
(l) List All Sensors
Enter selection or (0) to quit: _

Bild 160: Remote Manager: Enclosure Information-Fenster

Das Untermenü bietet Ihnen folgende Funktionen:

System Eventlog	Ruft das Menü *System Eventlog* auf (siehe Abschnitt „System Event-Log“ auf Seite 323).
Temperature	Informationen über die Temperatur-Sensoren und deren Status anzeigen.
Voltages/Current	Informationen über die Spannungs- und Strom-Sensoren und deren Status anzeigen.
Fans	Informationen über die Lüfter und deren Status anzeigen.
Power Supplies	Informationen über die Netzteile und deren Redundanz-Status anzeigen.
Door Lock	Informationen anzeigen, ob Front oder Gehäuse geöffnet sind.
CPU Sensors	Prozessor(en) des Servers lokalisieren.
Component Status	Detail-Informationen zu allen Sensoren anzeigen, die über eine PRIMERGY Diagnostic LED verfügen.
List all Sensors	Detail-Informationen zu allen Sensoren anzeigen.

Tabelle 12: Menü Enclosure Information

System Event-Log

Wenn Sie im Untermenü *Enclosure Information...* den Menüpunkt *System Eventlog* auswählen, erhalten Sie das folgende Menü:

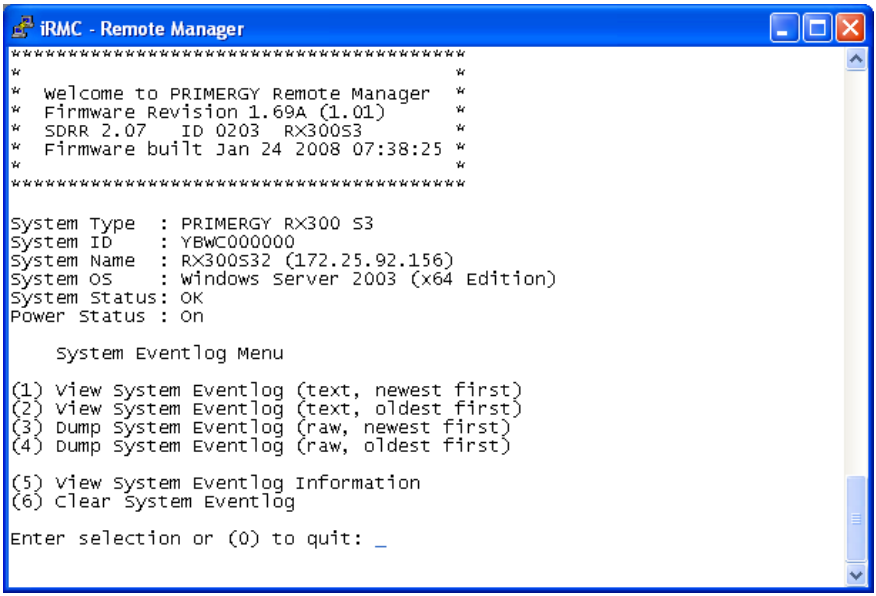

iRMC - Remote Manager
****
*   *
* Welcome to PRIMERGY Remote Manager   *
* Firmware Revision 1.69A (1.01)   *
* SDRR 2.07   ID 0203 RX300S3   *
* Firmware built Jan 24 2008 07:38:25 *
*   *
****
System Type : PRIMERGY RX300 S3
System ID   : YBWC000000
System Name : RX300S32 (172.25.92.156)
System OS   : Windows Server 2003 (x64 Edition)
System Status: OK
Power Status : On
System Eventlog Menu
(1) View System Eventlog (text, newest first)
(2) View System Eventlog (text, oldest first)
(3) Dump System Eventlog (raw, newest first)
(4) Dump System Eventlog (raw, oldest first)
(5) View System Eventlog Information
(6) Clear System Eventlog
Enter selection or (0) to quit: _

Bild 161: Remote Manager: System Eventlog-Fenster

Das Untermenü bietet Ihnen folgende Funktionen:

View System Eventlog (text, newest first)	Der Inhalt des Event-Log wird in lesbarer Form und chronologischer Reihenfolge am Bildschirm ausgegeben (der jüngste Eintrag zuerst).
View System Eventlog (text, oldest first)	Der Inhalt des Event-Log wird in lesbarer Form und chronologischer Reihenfolge am Bildschirm ausgegeben (der älteste Eintrag zuerst).
Dump System Eventlog (raw, newest first)	Der Inhalt des Event-Log wird in chronologischer Reihenfolge ausgeschrieben (der jüngste Eintrag zuerst).
Dump System Eventlog (raw, oldest first)	Der Inhalt des Event-Log wird in chronologischer Reihenfolge ausgeschrieben (der älteste Eintrag zuerst).
View System Eventlog Information	Informationen zum Event-Log.
Clear System Eventlog	Der Inhalt des Event-Log wird gelöscht.

Tabelle 13: Menü System Eventlog

8.2.10 Service Processor - IP-Parameter, Identifizierungs-LED und Reset des iRMC

Wenn Sie im Hauptmenü den Menüpunkt *Service Processor...* auswählen, erhalten Sie das folgende Menü:

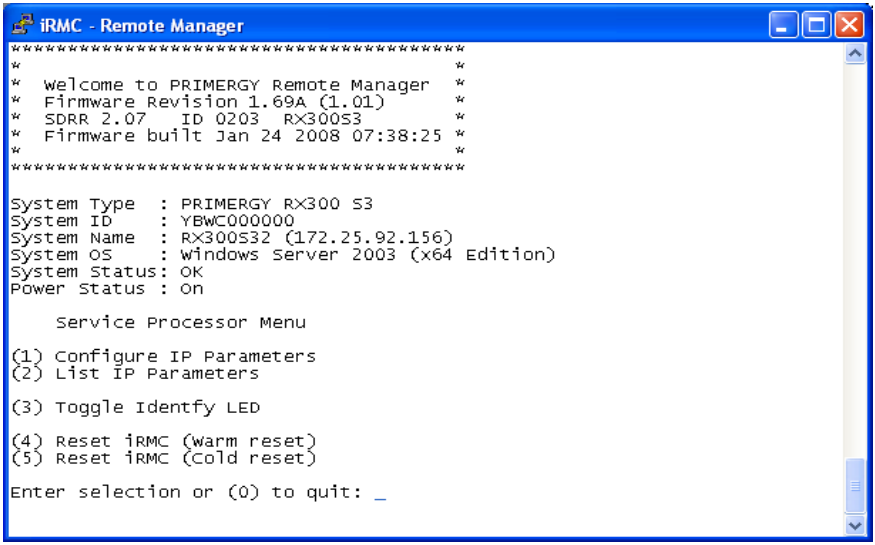

iRMC - Remote Manager
****
*   *
* Welcome to PRIMERGY Remote Manager   *
* Firmware Revision 1.69A (1.01)   *
* SDRR 2.07   ID 0203 RX300S3   *
* Firmware built Jan 24 2008 07:38:25 *
*   *
****
System Type : PRIMERGY RX300 S3
System ID   : YBWC000000
System Name : RX300S32 (172.25.92.156)
System OS   : Windows Server 2003 (x64 Edition)
System Status: OK
Power Status : On
Service Processor Menu
(1) Configure IP Parameters
(2) List IP Parameters
(3) Toggle Identfy LED
(4) Reset iRMC (warm reset)
(5) Reset iRMC (Cold reset)
Enter selection or (0) to quit: _

Bild 162: Remote Manager: Service Processor-Fenster

Das Untermenü bietet Ihnen folgende Funktionen:

Configure IP Parameters	IP-Adresse, Subnet-Maske und Standard-Gateway konfigurieren. Außerdem können Sie einstellen, ob DHCP aktiviert werden soll.
List IP Parameters	IP-Einstellungen anzeigen.
Toggle Identify LED	PRIMERGY Identifizierungs-LED ein-/ausschalten.
Reset iRMC (Warm reset)	Reset des iRMC durchführen. Die Verbindung wird beendet. Es werden nur die Schnittstellen neu initialisiert.
Reset iRMC (Cold reset)	Reset des iRMC durchführen. Die Verbindung wird beendet. Der iRMC wird komplett neu initialisiert.

Tabelle 14: Menü Service Processor

Es wird empfohlen, nach einem *Reset iRMC (Cold Reset)* oder *Reset iRMC (Warm Reset)* den Server neu zu starten (siehe Seite 214).

8.2.11 Console Redirection (EMS/SAC) - Text-Konsolumleitung starten

Unter dem Menüpunkt *Console Redirection (EMS/SAC)* des Hauptmenüs können Sie die Text-Konsolumleitung starten.

Die Text basierte Console Redirection funktioniert via LAN nur mit Serial 1.

Falls die Console redirection auch bei laufendem Betriebssystem genutzt werden soll, muss der *Serial 1Multiplexer* auf *System* konfiguriert sein.

8.2.12 Start a Command Line shell... - SMASH CLP Shell starten

Unter dem Menüpunkt *Start a Command Line shell...* des Hauptmenüs können Sie eine SMASH CLP Shell starten. SMASH CLP ist die Abkürzung für „**S**ystems **M**anagement **A**rchitecture“ for **S**erver **H**ardware **C**ommand **L**ine **P**rotocol“. Dieses Protokoll ermöglicht eine Verbindung zwischen der Management-Station und dem verwalteten Server auf Basis von Telnet oder SSH. Näheres zu SMASH CLP finden Sie im Abschnitt „Command Line Protocol (CLP)“ auf Seite 328.

Wenn Sie im Hauptmenü den Menüpunkt *(s) Start a Command Line shell...* auswählen, wird das folgende Fenster angezeigt:

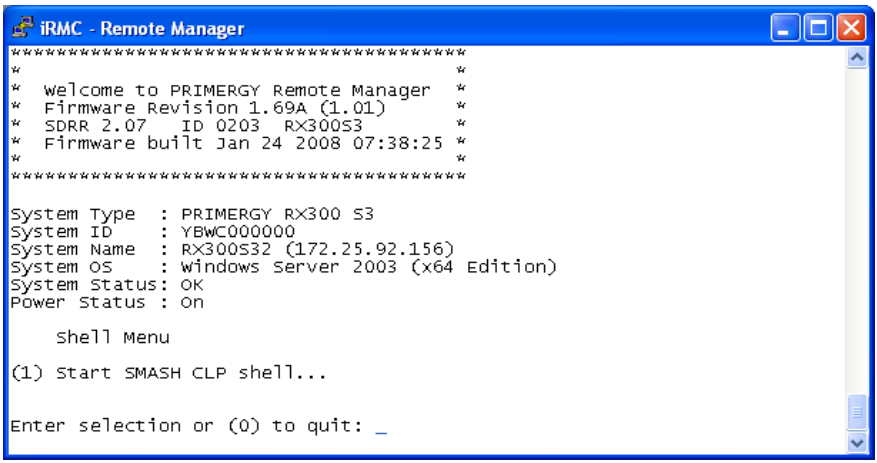

iRMC - Remote Manager
****
* Welcome to PRIMERGY Remote Manager *
* Firmware Revision 1.69A (1.01) *
* SDRR 2.07 ID 0203 RX300S3 *
* Firmware built Jan 24 2008 07:38:25 *
****
System Type : PRIMERGY RX300 S3
System ID : YBWC000000
System Name : RX300S32 (172.25.92.156)
System OS : Windows Server 2003 (x64 Edition)
System Status: OK
Power Status : On
Shell Menu
(1) Start SMASH CLP shell...
Enter selection or (0) to quit: _

Bild 163: Remote Manager: Start a SMASH CLP shell...-Fenster

► Wählen Sie *(1) Start a SMASH CLP shell...*, um die SMASH CLP Shell zu starten.

8.2.13 Command Line Protocol (CLP)

Der iRMC unterstützt verschiedene Text-basierte Benutzerschnittstellen, so genannte Benutzer-Shells, die für die einzelnen Benutzer unterschiedlich konfiguriert werden können.

Die Initiative **S**ystem **M**anagement **A**rchitecture for **S**erver **H**ardware (SMASH) definiert eine Reihe von Spezifikationen mit folgenden Zielen:

– Bereitstellung standardisierter Schnittstellen für das Management heterogener Rechnerlandschaften.

– Bereitstellung eines Architektur-Framework mit einheitlichen Schnittstellen, Hardware- und Software-Erkennung, Resource Addressing und Datenmodellen.

Weitere Informationen über SMASH finden unter folgendem Link:

http://www.dmtf.org/standards/smash

SMASH CLP-Syntax

SMASH CLP spezifiziert eine allgemeine Kommandozeilen-Syntax und Meldungsprotokoll-Semantik für das Management von Rechnern im Internet sowie im Umfeld von Unternehmen und Service Providern. Detaillierte Informationen zum SMASH CLP finden Sie in dem DMTF Dokument „Server Management Command Line Protocol Specification (SM CLP)DSP0214“.

Die allgemeine Syntax des CLP lautet wie folgt:

```
<verb> [<options>] [<target>] [<properties>]
```

<verb>

Verben spezifizieren, welches Kommando oder welche Aktion auszuführen ist. Die Liste der Verben beschreibt z. B. folgende Tätigkeiten:

– Daten generieren (*set*) und wiedergewinnen (*show*)

– Status eines Ziels ändern (*reset*, *start*, *stop*)

– aktuelle Sitzung steuern (*cd*, *version*, *exit*)

– Informationen zu Kommandos liefern (*help*)

In iRMC-Systemen ermöglicht außerdem das Verb *oemfujitsu* die Nutzung spezieller OEM-Kommandos.

<options>

(Kommando-)Options legen die Einzelheiten zur Aktion oder zum Verhalten eines Verbs fest. Options dürfen in einer Kommandozeile unmittelbar hinter dem Verb stehen und müssen immer mit einem vorangehenden Bindestrich („-“) angegeben werden.

Mithilfe von Options können Sie z.B.

- das Ausgabeformat festlegen,
- die rekursive Ausführung des Kommandos zulassen,
- die Version des Kommandos anzeigen lassen oder
- Hilfe-Informationen anfordern.

<target>

<target> spezifiziert die Adresse oder den Pfad des von dem Kommando zu manipulierenden Objekts, d.h. des Kommandoziels. Dies kann ein einzelnes überwachtes Element (Managed Element) sein, wie z.B. eine Festplatte, eine Netzkarte (Network Interface Card, NIC), oder das Administrationsprogramm (Management Assistance Program, MAP) selbst. Als mögliches Ziel kommen aber u.a. auch Services infrage, wie beispielsweise ein Transport-Service.

Unter einem <target> lassen sich mehrere Managed Elements zusammenfassen, deren Verwaltung vom Administrationsprogramm unterstützt wird, z.B. das System als Ganzes.

Pro Kommando darf nur ein einziges <target> angegeben werden.

<properties>

<properties> beschreiben die Eigenschaften des Kommandoziels, die zur Ausführung des Kommandos erforderlich sind. So identifizieren die <properties> über die Klasse des Kommandoziels die Properties im Zielobjekt, deren Werte vom Kommando ermittelt oder modifiziert werden.

Benutzerdaten im CLP (Überblick)

Die Daten innerhalb des CLP sind hierarchisch angeordnet. Mithilfe des Kommandos *cd* können Sie innerhalb dieser Struktur navigieren.

Bild 164 gibt einen Überblick über die Benutzerdaten im CLP. Die Namen in den Rechtecken bezeichnen Kommandoziele. Auf jeder Ebene der Hierarchie zeigt das Kommando bzw. Verb *show* die verfügbaren Ziele (Targets), Properties und Verben an.

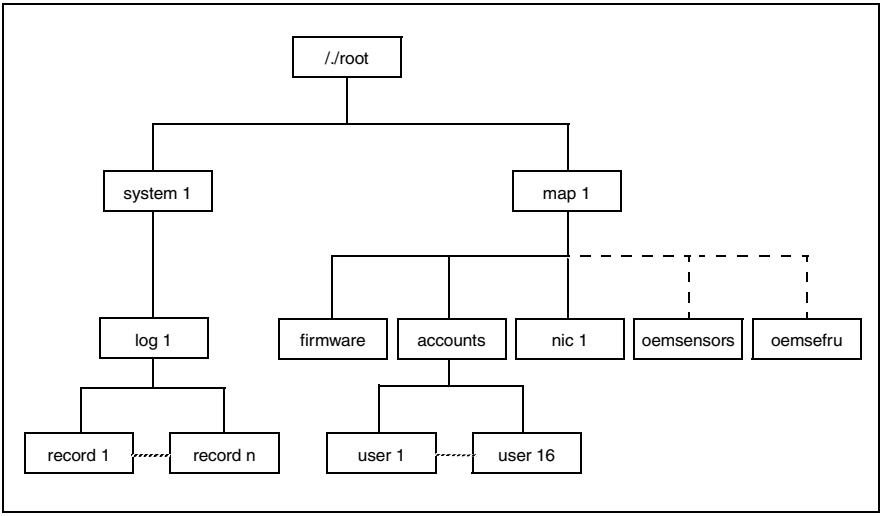


Bild 164: Struktur der Benutzerdaten in SMASH CLP

Hierarchie der CLP-Kommandos

Tabelle 15 auf Seite 331 gibt einen Überblick über die Hierarchie der CLP-Kommandos.

Verb / Target	Properties	Comment	cd	show	help	exit	version	set	reset	start	stop	load	oemfsc
/./		Root	X	X	X	X	X						
system1													
map1													
system1	name	Host System	X	X	X	X	X		System	PON	POFF		
	enabledstate												
...log1		Event Log (SEL)	X	X	X	X	X		iRMC				X
....record<n>	number	Single SEL entry	X	X	X	X	X		iRMC				X
	date												
	time												
	sensordescription												
	eventdescription												
	eventdirection												
map1	name	iRMC	X	X	X	X	X		iRMC				X
...firmware	version	iRMC FW	X	X	X	X	X		iRMC			X	X
...accounts		Accounts	X	X	X	X	X	X	iRMC				X
.....user<n>	username	User	X	X	X	X	X	X	iRMC				X
	password												
	group												
...nic1	networkaddress	LAN	X	X	X	X	X	X	iRMC				X
	oemfsc_nonvol_networkaddress												
	oemfsc_mask												
	oemfsc_nonvol_mask												
	oemfsc_gateway												
	oemfsc_nonvol_gateway												
	oemfsc_dhcp_enable												
	oemfsc_nonvol_dhcp_enable												
	oemfsc_vsi_path												
	oemfsc_vsi_server												
	oemfsc_vsi_permission												
	oemfsc_vsi_sustain												
...oemfsc_sensors		OEM Sensors	X	X	X	X	X		iRMC				X
....oemfsc_sensor_num<n>lun<m>	oemfsc_reading	Single Sensor	X	X	X	X	X		iRMC				X
	oemfsc_status												
	oemfsc_sensortype												
	oemfsc_readingtype												
...oemfsc_frus		FRU	X	X	X	X	X		iRMC				X
....oemfsc_fru_devid<n>lun<m>	oemfsc_description	Single FRU	X	X	X	X	X		iRMC				X

Tabelle 15: Hierarchie der CLP-Kommandos

9 iRMC via Server Configuration Manager konfigurieren

Dieses Kapitel beschreibt, wie Sie mithilfe des ServerView Configuration Managers

– den iRMC konfigurieren (ab Seite 346),

– Benutzerkennungen am iRMC konfigurieren und verwalten (ab Seite 361),

– einen Directory Service am iRMC konfigurieren (ab Seite 367).

Dabei können Sie den iRMC wahlweise lokal am verwalteten Server oder via ServerView Operations Manager (im Folgenden kurz: Operations Manager) vom Remote-Arbeitsplatz aus konfigurieren.

Voraussetzung:

Auf dem verwalteten Server sind die aktuellen ServerView-Agenten installiert.

Für den Zugang zur Server Configuration Manager-Funktionalität bieten sich folgende Möglichkeiten:

– Lokal am verwalteten Server über den ServerView Installation Manager (im Folgenden kurz Installation Manager).

– Lokal am verwalteten Windows-basierten Server über das Windows Start-menü.

  Diese Funktion wird nur für Server unterstützt, auf denen die ServerView-Agenten für Windows installiert sind.

– Am Remote-Arbeitsplatz über die grafische Oberfläche des Operations Managers.

  Diese Funktion wird nur für Server unterstützt, auf denen die ServerView-Agenten für Windows installiert sind.

9.1 Systemkonfiguration starten

Nachfolgend ist beschrieben, wie Sie den Server Configuration Manager über den ServerView Installation Manager, das Windows Startmenü und den ServerView Operations Manager aufrufen.

Die Benutzeroberflächen der einzelnen Server Configuration Manager-Varianten unterscheiden sich geringfügig im Layout, sind aber funktionell identisch.

Bei der Beschreibung der Server Configuration Manager-Dialoge zur Konfiguration des iRMC (siehe ab Seite 346) sind die Dialoge der Server Configuration Manager-Variante dargestellt, die Sie über den Operations Manager aufrufen.

9.1.1 Server Configuration Manager über den Installation Manager aufrufen

Den Server Configuration Manager können Sie über den Installation Manager aufrufen. Die Konfiguration via Installation Manager ist bei der Installation des Servers von Bedeutung. Der Installation Manager stellt den Server Configuration Manager sowohl im Rahmen der Installationsvorbereitung als auch als eigenes Wartungsprogramm zur Verfügung. Der Installation Manager ist beschrieben im Handbuch „ServerView Installation Manager“.

9.1.2 Server Configuration Manager über das Windows Startmenü aufrufen

Bei Windows-basierten Servern können Sie den Server Configuration Manager auch über das Windows Startmenü aufrufen.

Gehen Sie hierbei wie folgt vor:

- Wählen Sie am verwalteten Server:
  Start – All Programs – Fujitsu – ServerView – Agents – Configuration Tools – System Configuration.

  Das Fenster *System Configuration* öffnet sich:

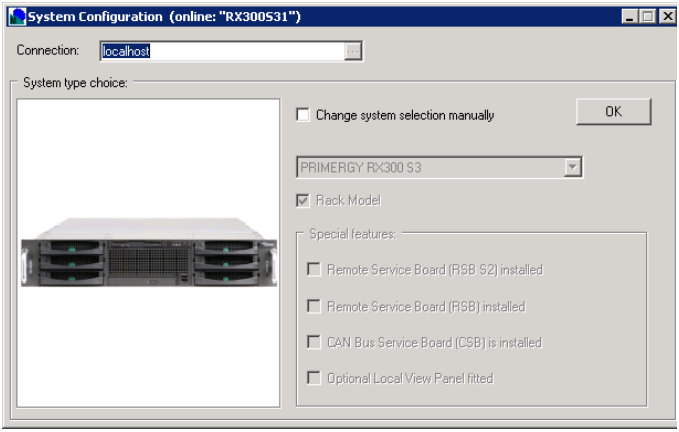


Bild 165: Fenster System Configuration

- Übernehmen Sie die voreingestellten Werte.
- Klicken Sie auf die Schaltfläche *OK*.

  Die 'Registerkarten-Ansicht' des Fensters *System Configuration* öffnet sich.

  Durch Klicken auf die Pfeile links neben der Leiste der Reiter können Sie in der Leiste nach links bzw. rechts blättern.

Einstellungen übernehmen

Um die in den einzelnen Registerkarten vorgenommenen Einstellungen zu übernehmen, verfahren Sie pro Registerkarte wie folgt:

- ► Klicken auf die Schaltfläche *Apply*.
- ► Klicken auf die Schaltfläche *Save Page*.

  Damit die Änderungen der Einstellungen wirksam werden, bootet der iRMC automatisch neu.

9.1.3 Server Configuration Manager über den Operations Manager aufrufen

Die Server Configuration Manager-Dialoge zur Konfiguration des iRMC stehen Ihnen auch über die grafische Oberfläche des Operations Managers zur Verfügung. Damit können Sie den iRMC des verwalteten Servers vom Remote-Arbeitsplatz aus via Web-Interface konfigurieren.

Gehen Sie wie folgt vor:

- Starten Sie den Operations Manager (siehe Handbuch „PRIMERGY ServerView Suite Operations Manager“).

  Das Startfenster des Operations Managers wird geöffnet:

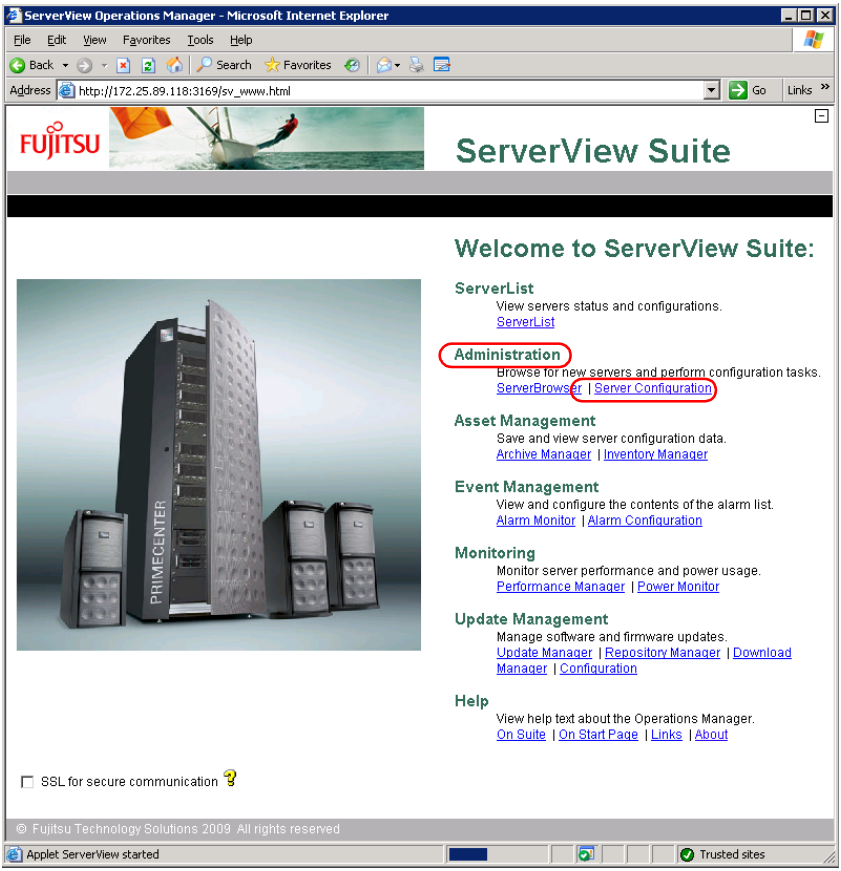

ServerView Operations Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://172.25.89.118:3169/sv_www.html
Go Links
FUJITSU
ServerView Suite
Welcome to ServerView Suite:
ServerList
View servers status and configurations.
ServerList
Administration
Browse for new servers and perform configuration tasks.
ServerBrowser | Server Configuration
Asset Management
Save and view server configuration data.
Archive Manager | Inventory Manager
Event Management
View and configure the contents of the alarm list.
Alarm Monitor | Alarm Configuration
Monitoring
Monitor server performance and power usage.
Performance Manager | Power Monitor
Update Management
Manage software and firmware updates.
Update Manager | Repository Manager | Download Manager | Configuration
Help
View help text about the Operations Manager.
On Suite | On Start Page | Links | About
SSL for secure communication
© Fujitsu Technology Solutions 2009. All rights reserved
Applet ServerView started
Trusted sites

Bild 166: Operations Manager: Startfenster

► Wählen Sie im Menu des Operations Manager-Startfensters unter *Administration* den Menü-Punkt *Server Configuration*.

Das folgende Fenster wird angezeigt (siehe Bild 167 auf Seite 339):

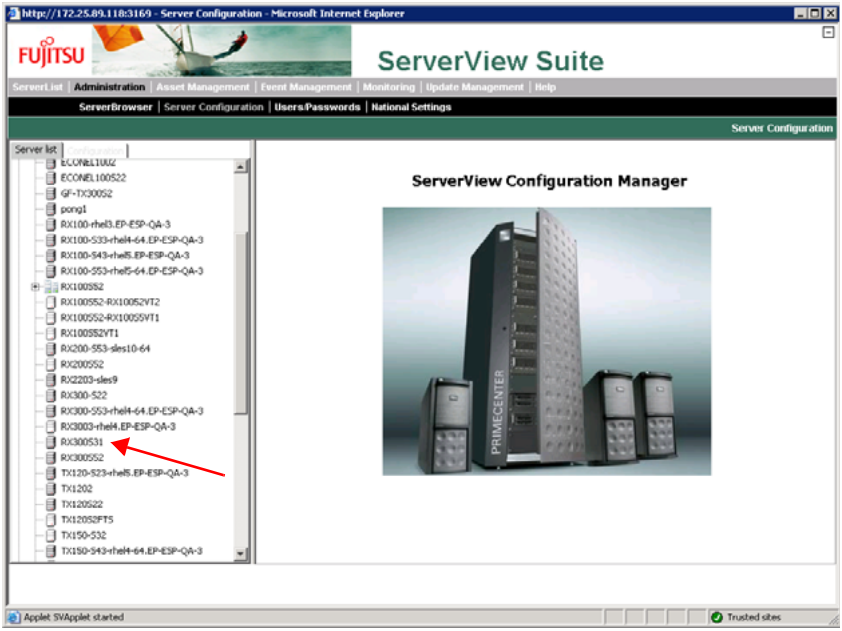

http://172.25.89.118:3169 - Server Configuration - Microsoft Internet Explorer
FUJITSU
ServerView Suite
ServerList | Administration | Asset Management | Event Management | Monitoring | Update Management | Help
ServerBrowser | Server Configuration | Users/Passwords | National Settings
Server Configuration
Server list
ServerView Configuration Manager
PRIMECENTER
Applet SVApplet started
Trusted sites

Bild 167: Operations Manager: Fenster Server Configuration - Registerkarte Server list (1)

► Klicken Sie im Strukturbaum der Registerkarte *Server list* auf den zu konfigurierenden Server.

Das folgende Fenster wird angezeigt (siehe Bild 168 auf Seite 340):

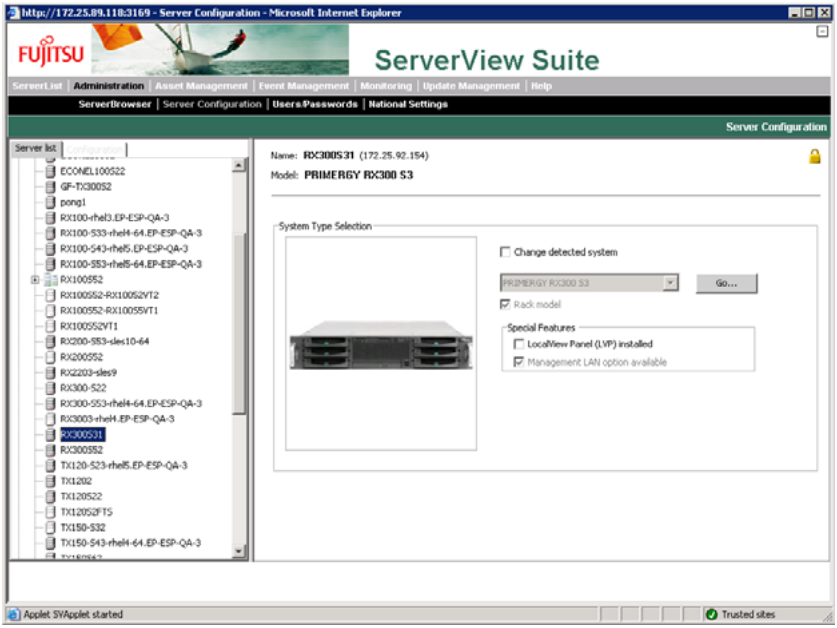


Bild 168: Operations Manager: Fenster Server Configuration - Registerkarte Server list (2)

► Spezifizieren Sie im rechten Bereich des Fensters die Details zum gewählten Server und bestätigen Sie mit *GO...* .

Es wird das folgende Fenster angezeigt, in dem der Dialog *Restart Options* aktiviert ist (siehe Bild 169 auf Seite 341):

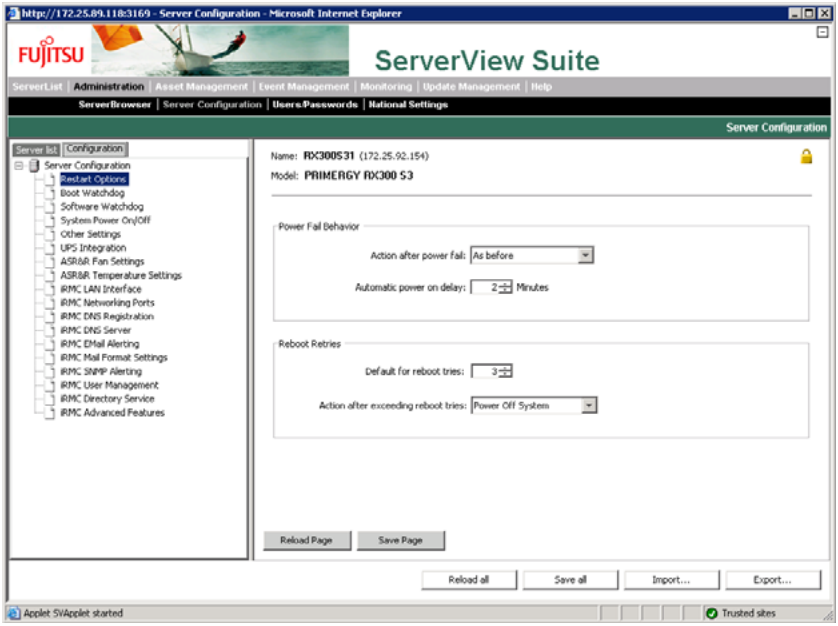


Bild 169: Operations Manager: Fenster Server Configuration - Registerkarte Configuration

► Klicken Sie im Navigationsbereich auf die gewünschten Funktion. Im rechten Bereich wird dann der zugehörige Dialog angeboten.

> **i** Im vorliegenden Handbuch sind nur die Dialoge beschrieben, die für die Konfiguration des iRMC sowie für die Benutzerverwaltung am iRMC relevant sind.

► Konfigurieren Sie Ihre Einstellungen und sichern Sie diese mit *Save Page* bzw. mit *Save all*.

> **i** Für jeden Server aktivieren Sie die konfigurierten Einstellungen wahlweise pro Dialog separat mit *Save Page* oder abschließend für die gesamte Konfiguration mit *Save all*.
>
> Mit *Reload Page* bzw. *Reload all* können Sie die Einstellungen auf die ursprünglichen Werte zurücksetzen.

> **i** Nach Abschluss einer Serverkonfiguration können Sie über die Registerkarte *Server list* weitere Server für eine Konfiguration auswählen.

9.2 ASR&R Fan Settings

Im Dialog *ASR&R Fan Settings* werden umfassende Informationen zu den Lüftern des verwalteten Servers angezeigt. Darüber hinaus können Sie für jeden Lüfter festlegen, ob der Server bei Ausfall des betreffenden Lüfters heruntergefahren werden soll.

► Wählen Sie *ASR&R Fan Settings*.

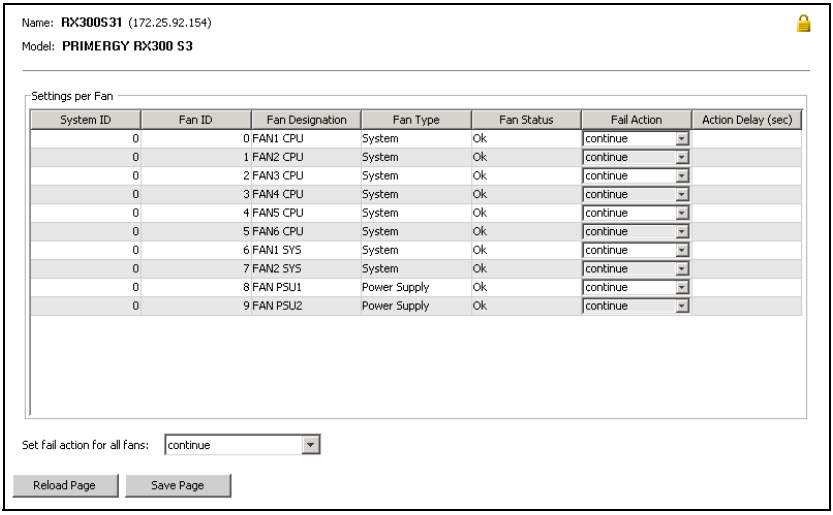

Name: RX300S31 (172.25.92.154)
Model: PRIMERGY RX300 S3
Settings per Fan
System ID
Fan ID
Fan Designation
Fan Type
Fan Status
Fail Action
Action Delay (sec)
0 0 FAN1 CPU System Ok continue
0 1 FAN2 CPU System Ok continue
0 2 FAN3 CPU System Ok continue
0 3 FAN4 CPU System Ok continue
0 4 FAN5 CPU System Ok continue
0 5 FAN6 CPU System Ok continue
0 6 FAN1 SYS System Ok continue
0 7 FAN2 SYS System Ok continue
0 8 FAN PSU1 Power Supply Ok continue
0 9 FAN PSU2 Power Supply Ok continue
Set fail action for all fans: continue
Reload Page
Save Page

Bild 170: Dialog ASR&R Fan Settings

► Konfigurieren Sie folgende Einstellungen:

Fail Action

Wählen Sie hier, ob der Server bei Ausfall des betreffenden Lüfters heruntergefahren werden soll.

Continue

Der Server wird nicht heruntergefahren.

Shutdown

Der Server wird heruntergefahren, sofern der Lüfter nach Ablauf der unter *Action Delay (sec)* festgelegten Zeitspanne weiterhin defekt ist.

Action Delay (sec)

Falls Sie unter *Fail Action* „Shutdown“ gewählt haben, können Sie hier eine Zeitspanne (in Sekunden) festlegen.

Der Server wird heruntergefahren, wenn der betreffende Lüfter nach Ablauf der angegebenen Zeitspanne weiterhin defekt ist.

Wenn Sie keinen Wert eintragen, wird der Server unmittelbar nach Ausfall des Lüfters heruntergefahren.

Set fail action for all fans

Hier können Sie für alle Lüfter einheitlich festlegen, ob der Server bei Ausfall eines Lüfters heruntergefahren werden soll:

Continue

Der Server wird heruntergefahren.

Shutdown

Der Server heruntergefahren, falls der ausgefallene Lüfter nach Ablauf der unter *Action Delay (sec)* festgelegten Zeitspanne weiterhin defekt ist.

9.3 ASR&R Temperature Settings

Im Dialog *ASR&R Temperature Settings* werden umfassende Informationen zu den Temperatur-Sensoren des verwalteten Servers angezeigt. Darüber hinaus können Sie für jeden Sensor festlegen, ob der Server bei Erreichen von kritischen Temperaturwerten abgeschaltet werden soll.

► Wählen Sie *ASR&R Temperature Settings*.

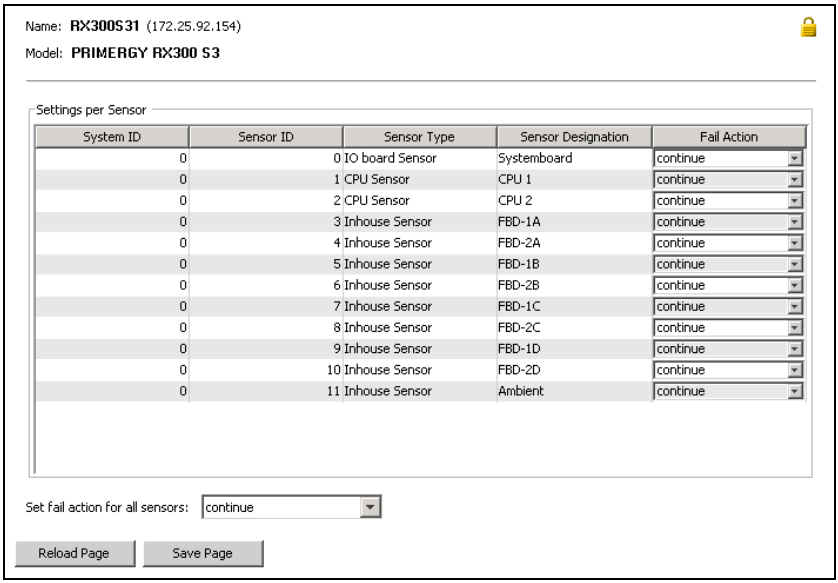

Name: RX300S31 (172.25.92.154)
Model: PRIMERGY RX300 S3
Settings per Sensor
System ID
Sensor ID
Sensor Type
Sensor Designation
Fail Action
0 0 IO board Sensor Systemboard continue
0 1 CPU Sensor CPU 1 continue
0 2 CPU Sensor CPU 2 continue
0 3 Inhouse Sensor FBD-1A continue
0 4 Inhouse Sensor FBD-2A continue
0 5 Inhouse Sensor FBD-1B continue
0 6 Inhouse Sensor FBD-2B continue
0 7 Inhouse Sensor FBD-1C continue
0 8 Inhouse Sensor FBD-2C continue
0 9 Inhouse Sensor FBD-1D continue
0 10 Inhouse Sensor FBD-2D continue
0 11 Inhouse Sensor Ambient continue
Set fail action for all sensors: continue
Reload Page
Save Page

Bild 171: Dialog ASR&R Temperature Settings

► Konfigurieren Sie folgende Einstellungen:

Fail Action

Wählen Sie hier, ob der Server bei Erreichen der kritischen Temperatur am ausgewählten Sensor heruntergefahren werden soll.

Continue

Der Server wird nicht heruntergefahren.

Shutdown

Der Server heruntergefahren.

Set fail action for all fans

Hier können Sie für alle Temperatur-Sensoren einheitlich festlegen, ob der Server bei Überschreiten der kritischen Temperatur heruntergefahren werden soll:

Continue

Der Server wird nicht heruntergefahren.

Shutdown

Der Server wird heruntergefahren.

9.4 iRMC LAN Interface - LAN-Einstellungen des iRMC konfigurieren

Im Dialog *iRMC LAN Interface* konfigurieren Sie die LAN-Einstellungen (Ethernet-Einstellungen) des iRMC.

ACHTUNG!

Kontaktieren Sie den zuständigen Netz-Administrator, bevor Sie die LAN-Einstellungen ändern.

Wenn Sie für den iRMC unzulässige LAN-Einstellungen konfigurieren, können Sie nur über eine Konfigurationssoftware, über die serielle Schnittstelle oder im BIOS wieder auf den iRMC zugreifen.

► Wählen Sie *iRMC LAN Interface*.

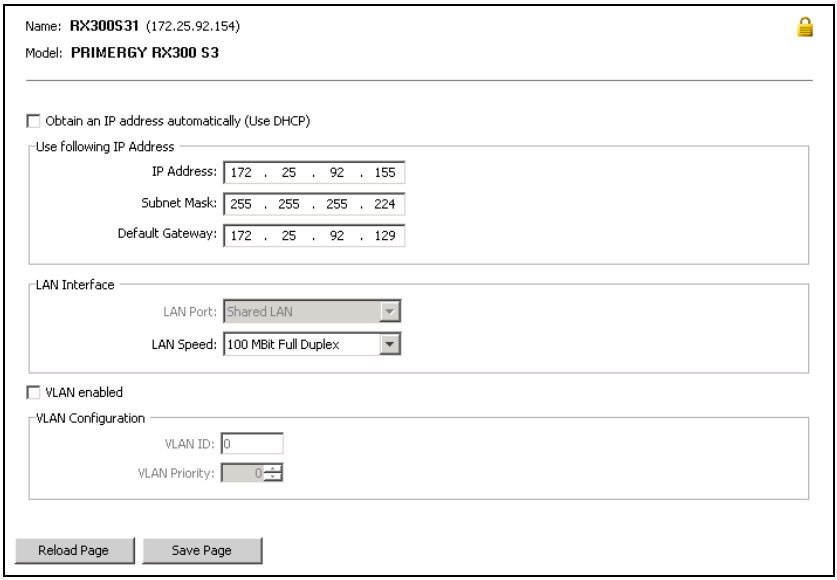

Name: RX300S31 (172.25.92.154)
Model: PRIMERGY RX300 S3
Obtain an IP address automatically (Use DHCP)
Use following IP Address
IP Address: 172 . 25 . 92 . 155
Subnet Mask: 255 . 255 . 255 . 224
Default Gateway: 172 . 25 . 92 . 129
LAN Interface
LAN Port: Shared LAN
LAN Speed: 100 MBit Full Duplex
VLAN enabled
VLAN Configuration
VLAN ID: 0
VLAN Priority: 0
Reload Page
Save Page

Bild 172: Dialog iRMC LAN Interface

► Konfigurieren Sie folgende Einstellungen:

Obtain an IP address automatically (Use DHCP)

Wenn Sie *Obtain an IP address automatically (Use DHCP)* aktivieren, erfragt der iRMC eigenständig seine LAN-Einstellungen bei einem DHCP-Server im Netz. In diesem Fall werden die Werte *IP address*, *Subnet mask* und *Default Gateway* automatisch gesetzt.

Aktivieren Sie DHCP nicht, wenn kein DHCP-Server verfügbar ist. Wenn Sie DHCP aktivieren und es ist kein DHCP-Server verfügbar, läuft der iRMC in eine Suchschleife (d.h. er sucht endlos nach einem DHCP-Server).

Die Nutzung der Dienste DHCP und DNS können Sie nach der Erstinstallation über die Dialoge *iRMC DHCP DNS Configuration* (siehe Seite 351) und *iRMC DNS Server Configuration* (siehe Seite 353) oder über die iRMC-Web-Oberfläche konfigurieren (siehe Abschnitt „Network Settings - LAN-Parameter konfigurieren“ auf Seite 239).
Standardmäßig wird bei der Erstinstallation für den iRMC folgende Bezeichnung an den DHCP-Server weitergegeben: *iRMC<letzte 3 Bytes der MAC-Adresse>*.

IP Address

Die Adresse des iRMC im LAN-Netzwerk. Sie unterscheidet sich von der IP-Adresse des verwalteten Servers.

Diese Eingabe wird nur ausgewertet, wenn DHCP nicht aktiviert ist (siehe *Obtain an IP address automatically (Use DHCP)*).

Subnet Mask

Subnet-Maske des iRMC im LAN-Netzwerk.

Diese Eingabe wird nur ausgewertet, wenn DHCP nicht aktiviert ist (siehe *Obtain an IP address automatically (Use DHCP)*).

Default Gateway

IP-Adresse des Default-Gateway für das LAN.

Diese Eingabe wird nur ausgewertet, wenn DHCP nicht aktiviert ist (siehe *Obtain an IP address automatically (Use DHCP)*).

LAN Speed

LAN-Geschwindigkeit. Zur Auswahl stehen:

- Auto Negotiation
- 100 MBit/s Full Duplex
- 100 MBit/s Half Duplex
- 10 MBit/s Full Duplex
- 10 MBit/s Half Duplex

Bei *Auto Negotiation* ermittelt der dem iRMC zugeordnete onboard LAN-Controller selbstständig die korrekte Übertragungsgeschwindigkeit und das Duplex-Verfahren des Netzwerkports, an den er angeschlossen ist.

VLAN enabled

Mithilfe dieser Option aktivieren Sie die VLAN-Unterstützung für den iRMC.

VLAN ID

VLAN-Identifier des virtuellen Netzes (VLAN), dem der iRMC angehört. Zulässiger Wertebereich: 1 ≤ *VLAN Id* ≤ 4094.

VLAN Priority

VLAN-Priorität (Benutzerpriorität) des iRMC in dem durch *VLAN Id* spezifizierten VLAN.
Zulässiger Wertebereich: 0 ≤ *VLAN Priority* ≤ 7 (Standardwert: 0).

9.5 iRMC Networking Ports - Ports und Netzdienste konfigurieren

Mit *iRMC Networking Ports* können Sie die Konfigurationseinstellungen für die Ports und Netzdienste einsehen und ändern.

ACHTUNG!

Für Ports, deren Eingabefelder bei Konfiguration an der iRMC-Web-Oberfläche deaktiviert sind (siehe Seite 243), wird eine Konfiguration nicht unterstützt. Die Konfigurierbarkeit der Ports kann nur an der iRMC-Web-Oberfläche verifiziert werden. Die voreingestellten Werte dürfen über den Server Configuration Manager bei der Erstkonfiguration nicht verändert werden.

► Wählen Sie die *iRMC Networking Ports*.

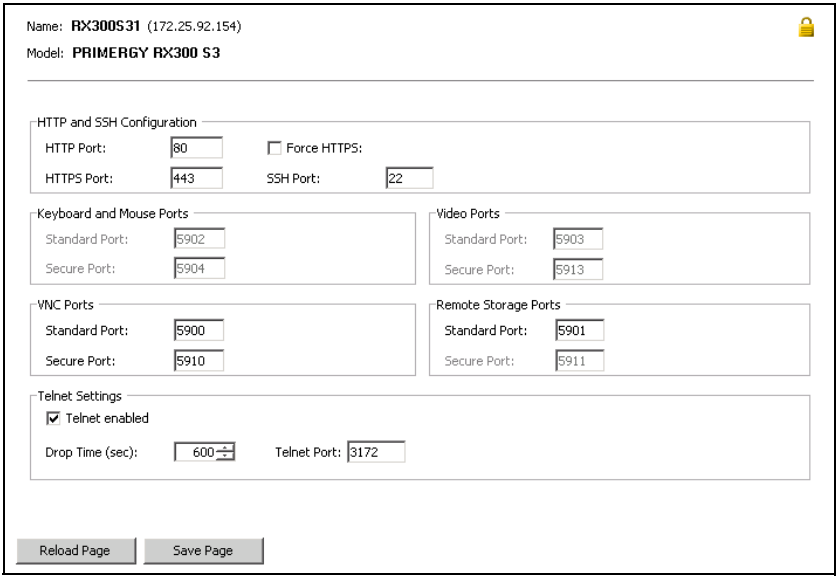


Bild 173: Dialog iRMC Networking Ports

► Konfigurieren Sie folgende Einstellungen:

HTTP Port

HTTP-Port des iRMC (nicht gesicherte Verbindung)

HTTPS Port

HTTPS-Port des iRMC (gesicherte Verbindung)

Force HTTPS

Wenn Sie *Force HTTPS* deaktivieren, können die Benutzer nur über den im Dialogfeld angegebenen HTTP-Port eine nicht-gesicherte Verbindung zum iRMC aufbauen.
Wenn Sie *Force HTTPS* aktivieren, können die Benutzer über den im Dialogfeld angegebenen HTTPS-Port eine gesicherte Verbindung zum iRMC aufbauen.

Sie können den Web-Zugang auch in der iRMC-Web-Oberfläche konfigurieren.
Wenn das SSL-Zertifikat ausgelaufen ist, wird am Web-Browser eine entsprechende Meldung ausgegeben.

SSH Port

SSH Port des iRMC

Video Ports - Standard Port

Video Port des iRMC, fest konfiguriert (Portnummer: 5903).

Video Ports - Secure Port

Sicherer Video Port des iRMC, fest konfiguriert (Portnummer: 5913).

VNC Ports - Standard Port

VNC Port des iRMC

VNC Ports - Secure Port

Sicherer VNC Port des iRMC

Remote Storage Ports - Standard Port

Remote Storage Port des iRMC

Telnet enabled

Wenn Sie *Telnet enabled* aktivieren, können die Benutzer über den im Dialogfeld angegebenen Telnet-Port eine Verbindung zum iRMC aufbauen.

Drop Time (sec)

Zeitspanne (in Sekunden), nach deren Verstreichen eine Telnet-Verbindung bei Inaktivität automatisch abgebaut wird.

Telnet Port

Telnet Port des iRMC. Das Eingabefeld wird nur dann angezeigt, wenn *Telnet enabled* aktiviert ist.

9.6 iRMC DNS Registration - Host-Namen für den iRMC konfigurieren

Im Dialog *iRMC DNS Registration* können Sie einen Host-Namen für den iRMC konfigurieren und somit „Dynamic DNS“ nutzen. Mit „Dynamic DNS“ können DHCP-Server die IP-Adresse und den Systemnamen einer Netzkomponente selbstständig zur besseren Identifikation an DNS-Server weitergeben.

► Wählen Sie *iRMC DNS Registration*.

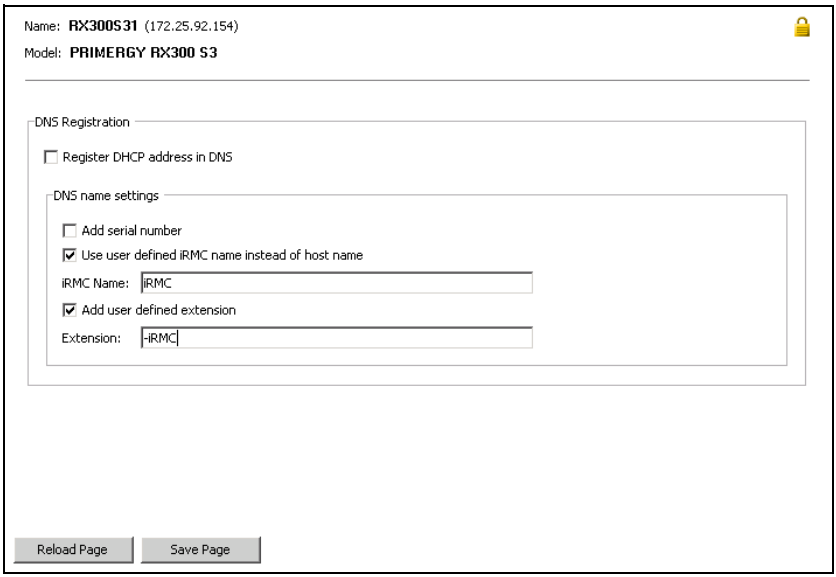


Bild 174: Dialog iRMC DNS Registration

► Konfigurieren Sie folgende Einstellungen:

Register DHCP address in DNS
: Aktiviert / deaktiviert die DHCP-Namensübergabe für den iRMC an den DHCP-Server.

Add serial number
: Dem DHCP-Namen für den iRMC werden rechts die letzten 3 Bytes der MAC-Adresse des iRMC angefügt.

Use user defined iRMC name instead of host name

Für den iRMC wird der im Dialogfeld *iRMC* Name spezifizierte iRMC-Name anstelle des Servernamens weitergegeben.

iRMC Name

iRMC-Name, der für den iRMC anstelle des Servernamens an DHCP weitergegeben wird.

Add user defined extension

Dem DHCP-Namen für den iRMC wird die im Dialogfeld *Extension* eingetragene Erweiterung angefügt.

Extension

Geben Sie hier eine Namenserweiterung für den iRMC ein.

9.7 iRMC DNS Server - DNS für den iRMC aktivieren

Im Dialog *iRMC DNS Server* können Sie für den iRMC den Domain Name Service (DNS) aktivieren. Sie können dann zur Konfiguration des iRMC symbolische DNS-Namen an Stelle von IP-Adressen verwenden.

► Wählen Sie *iRMC DNS Server*.

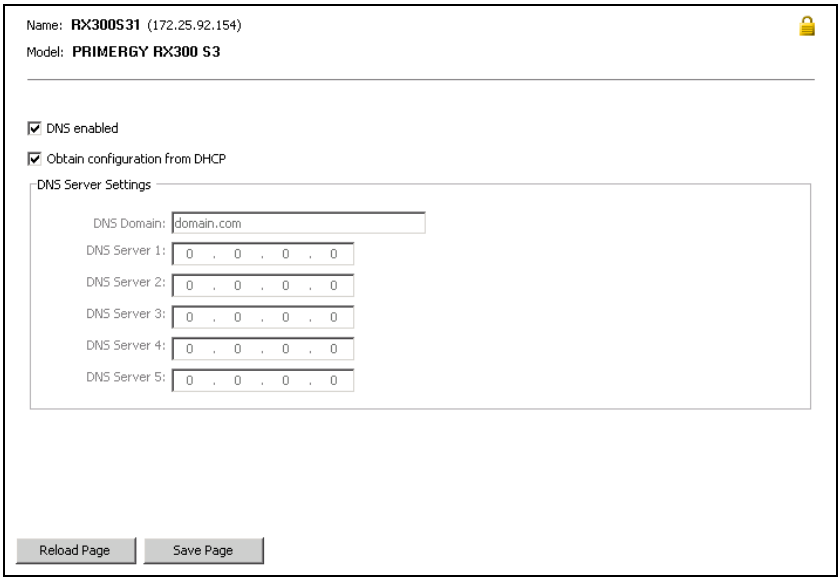

Name: RX300S31 (172.25.92.154)
Model: PRIMERGY RX300 S3
DNS enabled
Obtain configuration from DHCP
DNS Server Settings
DNS Domain: domain.com
DNS Server 1: 0 . 0 . 0 . 0
DNS Server 2: 0 . 0 . 0 . 0
DNS Server 3: 0 . 0 . 0 . 0
DNS Server 4: 0 . 0 . 0 . 0
DNS Server 5: 0 . 0 . 0 . 0
Reload Page
Save Page

Bild 175: iRMC DNS Server

► Konfigurieren Sie folgende Einstellungen:

DNS enabled
Aktiviert / deaktiviert DNS für den iRMC.

Obtain DNS configuration from DHCP
Wenn Sie diese Option aktivieren, werden die IP-Adressen der DNS-Server automatisch vom DHCP-Server übernommen.
In diesem Fall werden bis zu fünf DNS-Server unterstützt.

Wenn Sie diese Einstellung nicht aktivieren, können Sie unter *DNS-Server 1* - *DNS-Server 5* bis zu fünf DNS-Serveradressen manuell eingeben.

DNS Domain

Wenn die Option *Obtain DNS configuration from DHCP* deaktiviert ist, geben Sie hier den Namen der Default-Domäne für Anfragen an den bzw. die DNS Server an.

DNS Server 1 .. 5

Wenn die Option *Obtain DNS configuration from DHCP* deaktiviert ist, können Sie hier die IP-Adressen von bis zu fünf der DNS-Servern angeben.

9.8 iRMC EMail Alerting - E-Mail-Weiterleitung konfigurieren

Im Dialog *iRMC EMail Alerting* konfigurieren Sie die Einstellungen für das Weiterleiten von E-Mails durch den iRMC.

► Wählen Sie *iRMC EMail Alerting*.

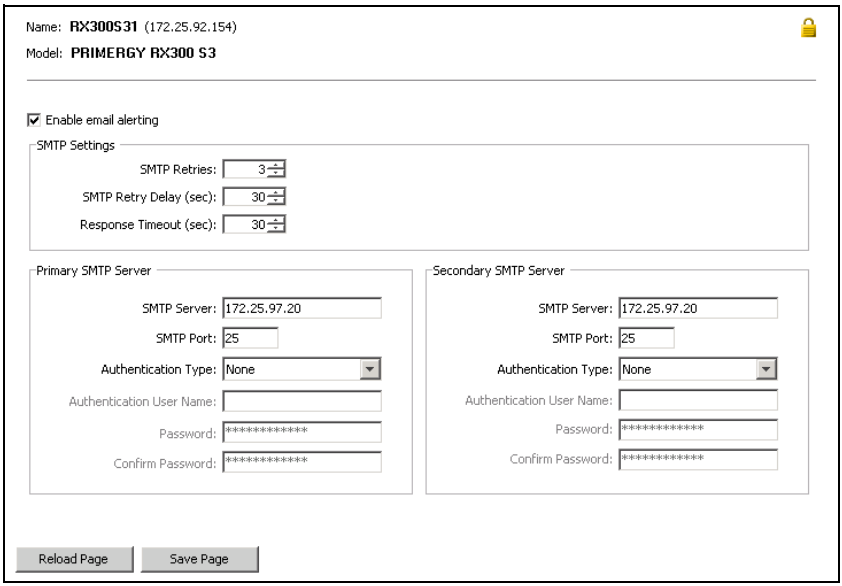


Bild 176: Dialog iRMC EMail Alerting

► Konfigurieren Sie folgende Einstellungen:

Enable email alerting
Aktivieren Sie diese Option.

SMTP Settings

Hier konfigurieren Sie die globalen E-Mail-Einstellungen.

SMTP Retries
Anzahl der SMTP-Retries

SMTP Retry Delay (sec)
Zeitraum zwischen den SMTP-Retries

Response Timeout (sec)
Timeout-Wert (in Sekunden) für SMTP-Antwort

Primary SMTP Server

Hier konfigurieren Sie die Einstellungen für den primären Mail Server (SMTP Server).

SMTP Server
IP-Adresse des primären Mail Servers.

Sie können für den iRMC den Domain Name Service (DNS) aktivieren (siehe „iRMC DNS Server - DNS für den iRMC aktivieren“ auf Seite 353). Anstelle der IP-Adresse können Sie dann einen symbolischen Namen angeben.

SMTP Port
SMTP Port des primären Mail Servers

Authentication Type
Einstellung für die Authentifizierung einer Verbindung des iRMC zum primären Mail Server:

- *None*
  Keinerlei Authentifizierung der Verbindung.
- *SMTP AUTH (RFC 2554)*
  Authentifizierung nach RFC 2554: SMTP Service Extension for Authentication

Authentication User Name
Benutzername für die Authentisierung beim primären Mail Server

Password
Geben Sie hier das Passwort für die Authentisierung beim primären Mail Server ein.

Confirm Password
Wiederholen Sie hier die Eingabe des Passworts.

Secondary SMTP Server

Hier konfigurieren Sie die Einstellungen für den sekundären Mail Server (SMTP-Server).

SMTP Server
IP-Adresse des sekundären Mail Servers.

> **i** Sie können für den iRMC den Domain Name Service (DNS) aktivieren (siehe „iRMC DNS Server - DNS für den iRMC aktivieren“ auf Seite 353). Anstelle der IP-Adresse können Sie dann einen symbolischen Namen angeben.

SMTP Port
SMTP Port des sekundären Mail Servers

Authentication Type
Einstellung für die Authentifizierung einer Verbindung des iRMC zum sekundären Mail Server:

- *None*
  Keinerlei Authentifizierung der Verbindung.
- *SMTP AUTH (RFC 2554)*
  Authentifizierung nach RFC 2554: SMTP Service Extension for Authentication

Authentication User Name
Benutzername für die Authentisierung beim sekundären Mail Server

Password
Geben Sie hier das Passwort für die Authentisierung beim sekundären Mail Server ein.

Confirm Password
Wiederholen Sie hier die Eingabe des Passworts.

9.9 iRMC Mail Format Settings - Mail-Format-abhängige Einstellungen

Im Dialog *iRMC Mail Format Settings* konfigurieren Sie die vom Mail-Format abhängigen Einstellungen. Das Mail-Format legen Sie pro Benutzer fest mithilfe des Dialogs *iRMC User Management* im *Edit existing user*-Fenster (siehe Seite 362).

Es werden die folgenden Mail-Formate unterstützt:

- Standard
- Fixed Subject
- ITS-Format
- Fujitsu REMCS Format

► Wählen Sie *iRMC Mail Format Settings*.

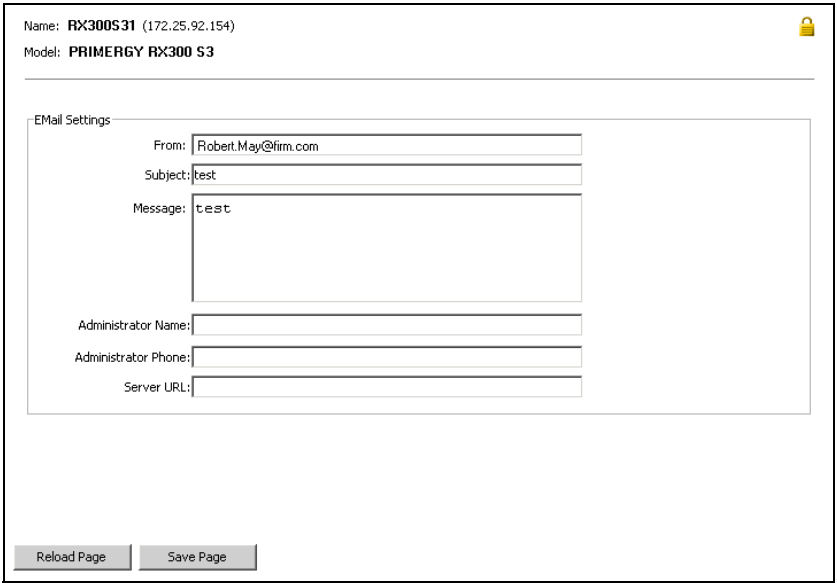


Bild 177: Dialog iRMC Mail Format Settings

► Konfigurieren Sie folgende Einstellungen. (Je nach Mail-Format sind nicht alle Eingabefelder aktiv.):

From

Identifikation des sendenden iRMC.
Aktiv bei allen Mail-Formaten.

> **i** Wenn in der hier eingegebenen Zeichenfolge ein „@“ enthalten ist, wird diese Zeichenfolge als gültige E-Mail-Adresse interpretiert. Andernfalls wird „admin@<ip-adresse>“ als gültige E-Mail-Adresse verwendet.

Subject

Fixed Subject der Alarmmeldung-E-Mails.
Aktiv nur bei Mail-Format *Fixed Subject* (siehe Seite 364).

Message

Art der Mitteilung (E-Mail).
Aktiv nur bei Mail-Format *Fixed Subject* (siehe Seite 364).

Administrator Name

Name des verantwortlichen Administrators (optional).
Aktiv nur bei Mail-Format *ITS* (siehe Seite 364).

Admininistrator Phone

Telefonnummer des verantwortlichen Administrators (optional).
Aktiv nur bei Mail-Format *ITS* (siehe Seite 364)

REMCS Id

Diese ID ist eine zusätzliche Indentifikation des Servers, ähnlich der Seriennummer.
Aktiv nur bei Mail-Format „Fujitsu REMCS-Format“ (siehe Seite 364).

Server URL

Eine URL, unter der der Server unter bestimmten Voraussetzungen zugänglich ist. Sie müssen die URL manuell eingeben.
Aktiv nur bei Mail-Format Standard (siehe Seite 364).

9.10 iRMC SNMP Alerting - SNMP-Alarm-Weiterleitung konfigurieren

Im Dialog *iRMC SNMP Alerting* können Sie die Einstellungen der SNMP-Alarmweiterleitung einsehen und konfigurieren.

Es wird die Weiterleitung von SNMP-Traps an bis zu sieben SNMP-Server unterstützt.

► Wählen Sie *iRMC SNMP Alerting*.

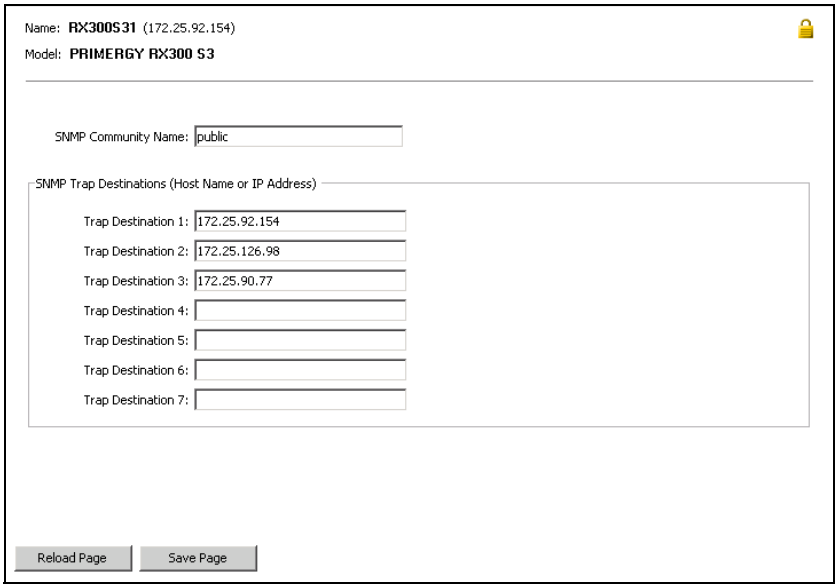


Bild 178: Dialog iRMC SNMP Alerting

► Konfigurieren Sie folgende Einstellungen:

SNMP Community Name
Name der SNMP-Community

SNMP Trap Destinations (Host name or IP address)
DNS-Namen oder IP-Adressen der Server, die dieser Community angehören und als Trap-Ziele (*Trap Destinations*) konfiguriert werden sollen.

9.11 iRMC User Management - Lokale Benutzerverwaltung am iRMC

Im Dialog *iRMC User Management* konfigurieren Sie die Einstellungen für die lokale Benutzerverwaltung am iRMC.

Der Dialog enthält eine tabellarische Übersicht über alle konfigurierten Benutzer: Pro Zeile werden die Daten eines konfigurierten Benutzers dargestellt.

Die Benutzerverwaltung am iRMC erfordert *Configure User Accounts*-Berechtigung.

Die User Id 1 („Null-User“) ist reserviert für den IPMI-Standard und steht deshalb nicht für die Benutzerverwaltung am iRMC zur Verfügung.

► Wählen Sie die *iRMC User Management*.

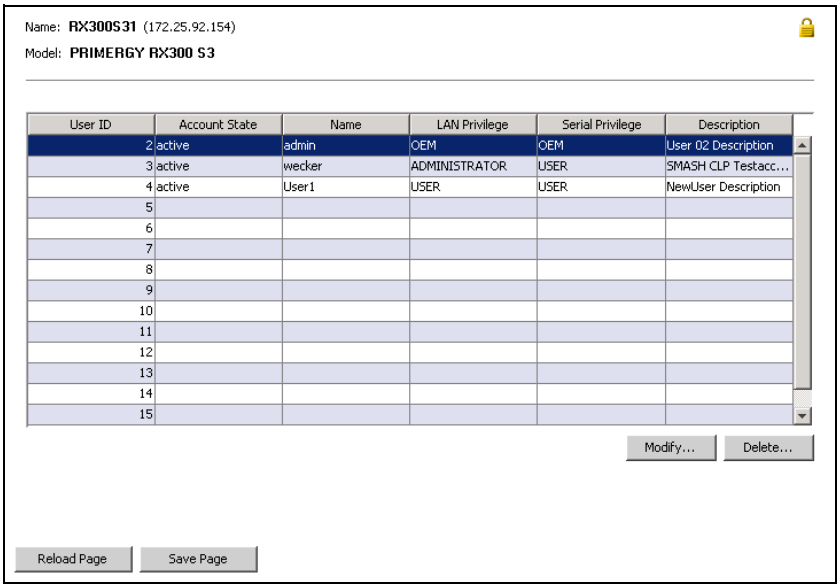


Bild 179: Dialog iRMC User Management

► Durch Auswählen eines Benutzers (Markieren der betreffenden Zeile) und Klicken auf die Schaltfläche *Delete...* können Sie diesen Benutzer nach nochmaliger Bestätigung löschen.

- Mit Doppel-Klick auf eine Zeile, deren User ID noch keinem Benutzers zugeordnet ist (leere Zeile) oder durch Auswählen einer solchen Zeile und Klicken auf die Schaltfläche *Modify ...* öffnen Sie ein leeres Fenster *Edit existing user* (mit Default-Einstellungen), in dem Sie einen neuen Benutzer konfigurieren können (siehe Bild 180).
- Mit Doppel-Klick auf die Zeile eines Benutzers oder durch Auswählen eines Benutzers und Klicken auf die Schaltfläche *Modify ...* öffnen Sie das Fenster *Edit existing user*, in dem Sie die Einstellungen des betreffenden Benutzers einsehen und/oder modifizieren können (siehe Bild 180).

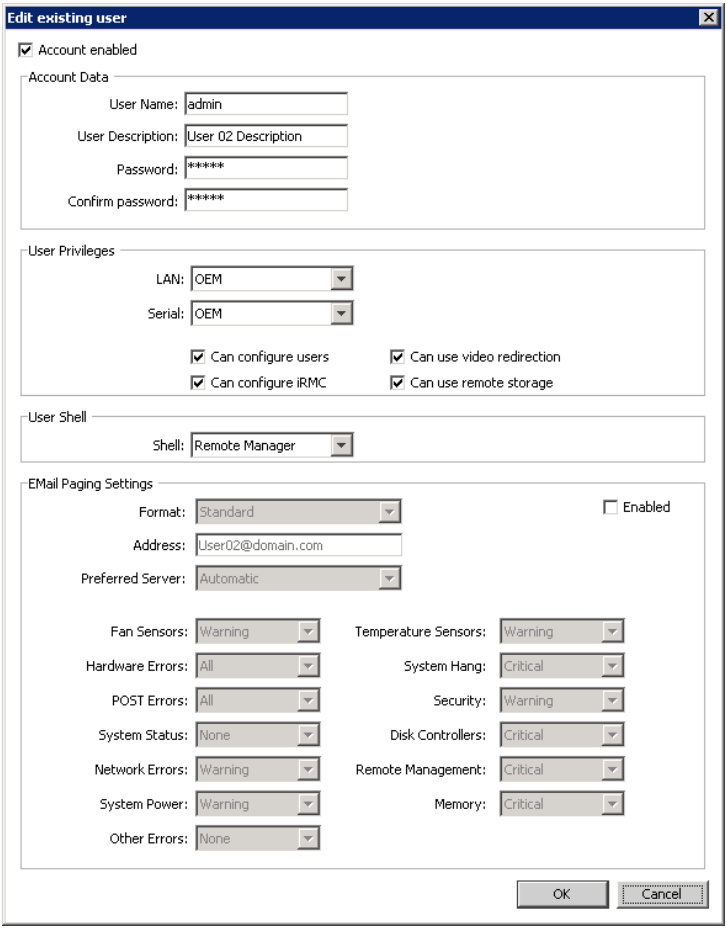


Bild 180: Dialog im Fenster Edit existing user

Account enabled
Durch deaktivieren der Option können Sie den Benutzer sperren.

Account Data

Hier konfigurieren Sie die Zugangsdaten des Benutzers.

User Name
Tragen Sie hier den Namen des Benutzers ein.

User Description
Zusätzliche Information zum Benutzer.

Password
Tragen Sie hier das Passwort des Benutzers ein.

Confirm Password
Wiederholen Sie hier zur Bestätigung die Eingabe des Passworts.

User Privileges

Hier konfigurieren Sie die Kanal-spezifischen Benutzerprivilegien sowie weiter Berechtigungen.

LAN
Ordnen Sie hier dem Benutzer eine Berechtigungsgruppe für den LAN-Kanal zu.
Zur Auswahl stehen:

- *User*
- *Operator*
- *Administrator*
- *OEM*

Zum Berechtigungsumfang der einzelnen Berechtigungsgruppen siehe Abschnitt „Benutzerberechtigungen“ auf Seite 62.

Serial
Ordnen Sie hier dem Benutzer eine Berechtigungsgruppe für den seriellen Kanal zu. Zur Auswahl stehen die gleichen Berechtigungsgruppen wie unter *LAN Privilege*.

Can configure users
Berechtigung zum Konfigurieren von lokalen Benutzerzugangsdaten.

Can configure iRMC
Berechtigung zum Konfigurieren der iRMC-Einstellungen.

Can use video redirection

Berechtigung zur Nutzung der Advanced Video Redirection (AVR) im „View Only“- und „Full Control“-Modus.

Can use remote storage

Berechtigung zur Nutzung der Remote Storage-Funktionalität.

User Shell

Hier wählen Sie die Benutzer-Shell aus.

Shell

Wählen Sie hier die gewünschte Benutzer-Shell aus.
Zur Auswahl stehen:

- *SMASH CLP*
  Siehe Abschnitt „Start a Command Line shell... - SMASH CLP Shell starten“ auf Seite 327.
- *Remote Manager*
  Siehe Kapitel „iRMC über Telnet/SSH (Remote Manager) bedienen“ auf Seite 307.
- *IPMI Basic Mode*
- *IPMI Terminal Mode*
- *None*

EMail Paging Settings

Hier konfigurieren Sie die Einstellungen für das E-Mail-Format sowie die globalen E-Mail-Einstellungen.

Format

Abhängig vom gewählten Mail-Format können Sie im Dialog *iRMC Email Format Settings* (siehe Seite 358) unterschiedliche Einstellungen vornehmen.

Folgende Mail-Formate stehen zur Verfügung:

- *Standard*
- *Fixed Subject*
- *ITS-Format*
- *Fujitsu REMCS Format*

Jeder Eventlog-Eintrag des iRMC wird einer bestimmten Paging-Gruppe zugeordnet.

Enabled

Hier stellen Sie ein, ob der Benutzer per E-Mail über die Systemzustände informiert werden soll.

Address

E-Mail-Adresse des Empfängers.

Preferred Server

Bevorzugter Mail Server.
Sie können wählen zwischen folgenden Optionen:

– *Automatic*

  Falls die E-Mail nicht sofort erfolgreich versendet werden kann, weil z.B. der erste Mail Server nicht verfügbar ist, wird E-Mail an den zweiten Mail Server gesendet.

– *Primary*

  Nur der als Primary SMTP Server (siehe Seite 356) konfigurierte SMTP Server wird als bevorzugter Mail Server verwendet.

– *Secondary*

  Nur der als Secondary SMTP-Server (siehe Seite 357) konfigurierte SMTP Server wird als bevorzugter Mail Server verwendet.

Fehler beim Versenden der E-Mail werden als Event Log gemeldet.

Im unteren Drittel des Fensters *Edit existing user* konfigurieren Sie System-Ereignisse, über die ein iRMC-Benutzer per E-Mail benachrichtigt werden soll (Paging Severity Configuration).

NONE

Die Benachrichtigungsfunktion für diese Paging-Gruppe ist deaktiviert.

WARNING

Der iRMC benachrichtigt Benutzer per E-Mail, wenn ein System-Event-Log-Eintrag den Status *WARNING* meldet.

Unter der Einstellung *WARNING* werden dem Benutzer zusätzlich auch System-Event-Log-Einträge mit dem Status *CRITICAL* gemeldet.

CRITICAL

Der iRMC benachrichtigt Benutzer per E-Mail, wenn ein System-Event-Log-Eintrag den Status *CRITICAL* meldet.

ALL

Der iRMC benachrichtigt Benutzer über jedes zu einem Eintrag in das System-Event-Log führende Ereignis in dieser Gruppe.

► Bestätigen Sie Ihre Einstellungen mit *OK*.

9.12 iRMC Directory Service - Directory Service konfigurieren

Im Dialog *iRMC Directory Service* konfigurieren Sie den iRMC für die globale Benutzerverwaltung über einen Directory Service (siehe Seite 68).

Derzeit werden LDAP-Zugriffe des iRMC für die Directory Services Microsoft Active Directory, Novell eDirectory und OpenLDAP unterstützt.

Die folgenden Zeichen sind in LDAP als Meta-Zeichen für Such-Strings reserviert: &, |, !, =, <, >, ~, :

Verwenden Sie diese Zeichen deshalb nicht als Bestandteil von Relative Distinguished Names (RDN).

► Wählen Sie *iRMC Directory Service*.

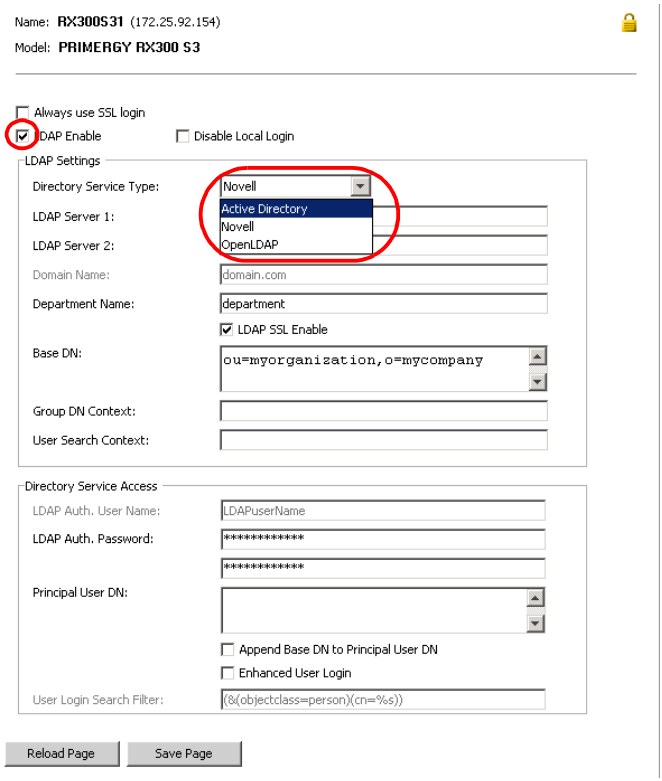


Bild 181: Dialog iRMC Directory Service

► Konfigurieren Sie die folgenden Einstellungen:

Always use SSL login

Diese Option ist nur relevant, wenn gleichzeitig LDAP deaktiviert ist.

Wenn Sie diese Option aktivieren, wird stets die HTTP SSL-gesicherte Login-Seite verwendet, auch wenn LDAP deaktiviert ist. Nur wenn Sie *Always use SSL Login* nicht aktivieren und außerdem LDAP deaktiviert ist, kommt eine über Digest Authentication Login gesicherte Maske zum Einsatz.

LDAP Enable

Mit dieser Option legen Sie fest, ob der iRMC via LDAP auf einen Directory Service zugreifen kann. Der Directory Service via LDAP kann nur genutzt werden, wenn *LDAP Enable* aktiviert ist

Wenn *LDAP Enable* aktiviert ist, wird die Login-Information (siehe Seite 182) immer SSL-verschlüsselt zwischen dem Web-Browser und dem iRMC übertragen.

Disable Local Login

Wenn Sie diese Option aktivieren, werden alle iRMC-lokalen Benutzerkennungen gesperrt, und nur die durch den Directory Service verwalteten Benutzkennungen sind gültig.

ACHTUNG!

Wenn die Option *Disable Local Login* aktiviert ist und außerdem die Verbindung zum Directory Service fehlschlägt, ist am iRMC kein Login mehr möglich.

► Wählen Sie unter *Directory Server Type* den gewünschten Directory Service.

Je nach gewähltem Directory Service werden unterschiedliche Eingabefelder angeboten:

– Zu *Active Directory* siehe „iRMC für Microsoft Active Directory konfigurieren“ auf Seite 369.

– Zu *Novell* und *OpenLDAP* siehe „iRMC für Novell eDirectory / OpenLDAP konfigurieren“ auf Seite 371.

9.12.1 iRMC für Microsoft Active Directory konfigurieren

Die in Bild 182 beispielhaft dargestellten Eingaben beziehen sich auf die im Abschnitt „iRMC-Benutzerverwaltung via Microsoft Active Directory“ auf Seite 80 dargestellten Beispiele und Abbildungen.

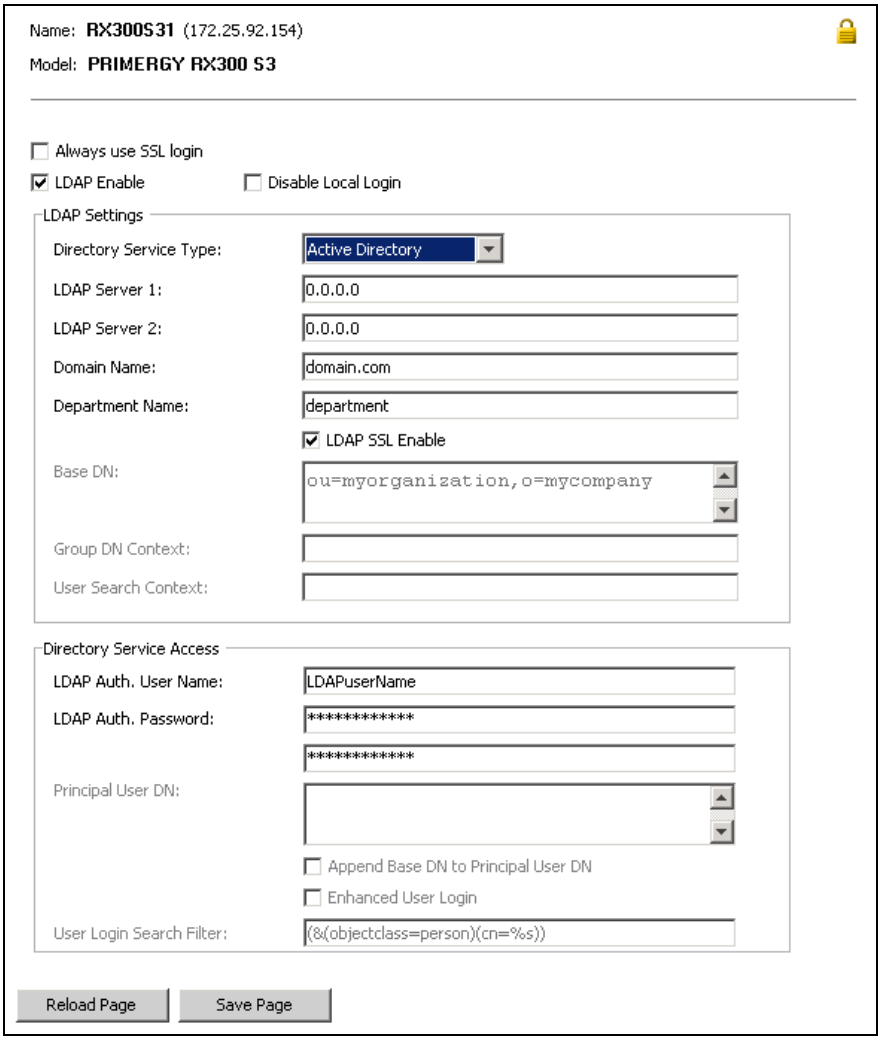


Bild 182: Dialog iRMC Directory Service (Microsoft Active Directory)

► Konfigurieren Sie die folgenden Einstellungen:

LDAP Server 1
IP-Adresse oder DNS-Name des zu verwendenden LDAP Directory Servers.

LDAP Server 2
IP-Adresse oder DNS-Name des LDAP Directory Servers, der als Backup Server geführt und bei Ausfall von *LDAP Server 1* als Directory Server herangezogen wird.

Domain Name
Vollständiger DNS Pfadname des Directory Servers.

Department Name
Abteilungsname. Der Abteilungsname wird im Directory Service zur Bestimmung der Benutzerrechte benötigt. Ein Benutzer kann für den Server der Abteilung X andere Rechte besitzen als für den Server der Abteilung Y (siehe auch Bild 17 auf Seite 73).

LDAP SSL Enable
Wenn Sie diese Option aktivieren, erfolgt der Datenaustausch zwischen iRMC und Directory Server SSL-verschlüsselt.

LDAP SSL Enable hat keinen Einfluss darauf, ob die Seiten der iRMC-Web-Oberfläche SSL-gesichert geöffnet werden oder nicht.

LDAP SSL Enable sollten Sie nur aktivieren, wenn ein Domain Controller-Zertifikat installiert ist.

Base DN
Base DN wird automatisch von *Domain Name* abgeleitet.

LDAP Auth. User Name, *LDAP Auth Password*
Diese Einstellungen unter sind zurzeit nicht relevant.
Die hier vorzunehmenden Einstellungen werden für die Alarmbenachrichtigung (Alerting) im Zusammenhang mit globalen Benutzerkennungen benötigt. Alerting wird derzeit jedoch nur für lokale Benutzerkennungen unterstützt.

9.12.2 iRMC für Novell eDirectory / OpenLDAP konfigurieren

Der Aufbau des Dialogs *Directory Service Configuration* ist für Novell eDirectory und OpenLDAP identisch.

Die in Bild 183 beispielhaft dargestellten Eingaben beziehen sich auf die im Abschnitt „iRMC-Benutzerverwaltung via Novell eDirectory“ auf Seite 98 dargestellten Beispiele und Abbildungen.

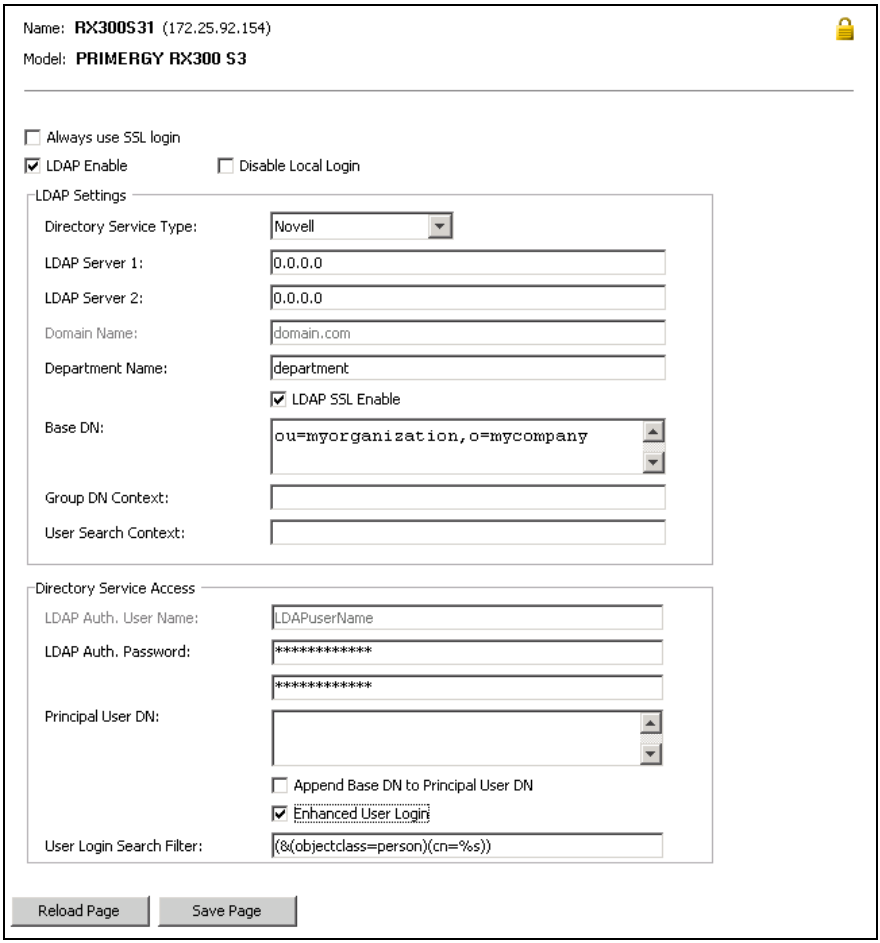


Bild 183: Dialog iRMC Directory Service

► Konfigurieren Sie die folgenden Einstellungen:

LDAP Server 1
IP-Adresse oder DNS-Name des zu verwendenden LDAP Directory Servers.

LDAP Server 2
IP-Adresse oder DNS-Name des LDAP Directory Servers, der als Backup Server geführt und bei Ausfall von *LDAP Server 1* als Directory Server herangezogen wird.

Department Name
Abteilungsname. Der Abteilungsname wird im Directory Service zur Bestimmung der Benutzerrechte benötigt. Ein Benutzer kann für den Server der Abteilung X andere Rechte besitzen als für den Server der Abteilung Y (siehe auch Bild 17 auf Seite 73).

LDAP SSL Enable
Wenn Sie diese Option aktivieren, erfolgt der Datenaustausch zwischen iRMC und Directory Server SSL-verschlüsselt.

LDAP SSL Enable hat keinen Einfluss darauf, ob die Seiten der iRMC-Web-Oberfläche SSL-gesichert geöffnet werden oder nicht.

LDAP SSL Enable sollten Sie nur aktivieren, wenn ein Domain Controller-Zertifikat installiert ist.

Base DN
Der *Base DN* ist der Full Distinguished Name des eDirectory bzw. OpenLDAP Servers und repräsentiert den Baum oder Teilbaum, in dem die OU (Organizational Unit) *iRMCgroups* enthalten ist. Dieser DN bildet den Ausgangspunkt für LDAP-Suchoperationen.

Group DN Context
Pfadname der OU *iRMCgroups* als Teilbaum von *Base DN*.

User Search Context
Pfadname der OU *Users* als Teilbaum von *Base DN*.

LDAP Auth. User Name
Generische iRMC-Benutzerkennung (Principal User), unter der der iRMC vom LDAP-Server die Benutzerberechtigungen der iRMC-Benutzer erfragt.

LDAP Auth. Password

Passwort, mit dem sich der Principal User beim LDAP-Server authentisiert, sowie Bestätigung des Passworts.

Principal User DN

Fully Distinguished Name der generischen iRMC-Benutzerkennung (Principal User), unter der der iRMC vom LDAP-Server die Benutzerberechtigungen der iRMC-Benutzer erfragt.

Append Base DN To Principal User DN

Wenn Sie diese Option aktivieren, brauchen Sie den Base DN unter *Principal User DN* nicht angeben. Es wird dann der unter *Base DN* spezifiziert Base DN verwendet.

Enhanced User Login

Erhöhte Flexibilität beim Benutzer-Login.

Wenn Sie *Enhanced User Login* auswählen, wird zusätzlich das Eingabefeld *User Login Search Filter* aktiviert, das mit dem Standard-Login-Suchfilter vorbelegt ist.

Beim Login wird der Platzhalter „%s“ durch die jeweilige globale Benutzerkennung ersetzt. Den Filter können Sie modifizieren, indem Sie z.B. anstatt „cn=“ ein anderes Attribut spezifizieren. Loginberechtigt am iRMC sind dann alle globalen Benutzkennungen, die den Bedingungen dieses Suchfilters genügen.

ACHTUNG!

Aktivieren Sie diese Option nur, wenn Sie mit der LDAP-Syntax vertraut sind. Wenn Sie versehentlich einen ungültigen Suchfilter spezifizieren und aktivieren, können sich Benutzer erst nach einer Deaktivierung der Option *Enhanced User Login* wieder unter einer globalen Benutzerkennung am iRMC einloggen.

9.13 iRMC Advanced Features - Remote Storage Server, License Key und HP SIM-Integration

Im Dialog *iRMC Advanced Features* können Sie folgende Aufgaben erledigen:

– IP-Adresse oder DNS-Namen eines Remote Storage Servers am iRMC abspeichern

– License Key für die Nutzung von Advanced Video Redirection und Remote Storage-Funktionalität eintragen.

– HP SIM-Integration deaktivieren bzw. aktivieren.

► Wählen Sie *iRMC Advanced Features*.

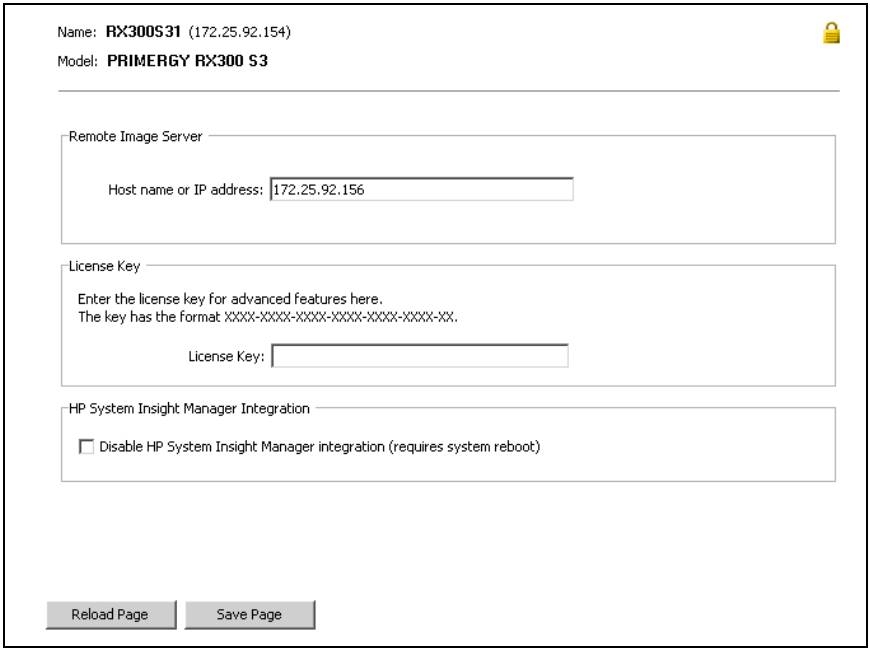

Name: RX300S31 (172.25.92.154)
Model: PRIMERGY RX300 S3
Remote Image Server
Host name or IP address: 172.25.92.156
License Key
Enter the license key for advanced features here.
The key has the format XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XX.
License Key:
HP System Insight Manager Integration
Disable HP System Insight Manager integration (requires system reboot)
Reload Page
Save Page

Bild 184: Dialog iRMC Advanced Features

► Konfigurieren Sie folgende Einstellungen:

Hostname or IP address
DNS-Name oder IP-Adresse des Computers, auf dem ein Remote Storage Server installiert ist.

License Key
Tragen Sie hier einen gültigen License Key für die Nutzung von Advanced Video Redirection und Remote Storage-Funktionalität ein.

Disable HP System Insight Manager integration ...
Aktivieren/deaktivieren Sie diese Option, um die HP SIM-Integration zu deaktivieren bzw. zu aktivieren.

Wenn die Option *Disable HP System Insight Manager Integration ...* deaktiviert ist, sendet der iRMC als Antwort auf eine nicht authentisierte XML-Anfrage des HP Insight Managers Identifizierungsinformationen an diesen zurück.

10 Firmware-Update

Dieses Kapitel informiert über folgende Themen:

– Firmware des iRMC (Überblick)

– Online-Firmware-Update

– Offline-Firmware-Update

– Emergency Flash

– Flash-Tools

Die aktuellen Firmware-Versionen erhalten Sie auf der *PRIMERGY ServerView Suite DVD 1* oder per manuellem Download aus der Download-Section des Web-Servers von Fujitsu Technology Solutions.

Die *PRIMERGY ServerView Suite DVD 1* können Sie alle zwei Monate aktuell beziehen.

Bevor Sie die Firmware aktualisieren, lesen Sie sorgfältig die mit der neuen Firmware gelieferte zusätzliche Dokumentation (vor allem die Readme-Dateien).

Um die aktualisierte Firmware zu aktivieren, ist ein Neustart des verwalteten Servers erforderlich.

ACHTUNG!

Beachten Sie beim Aktualisieren der Firmware, dass ein einwandfreies Funktionieren der Firmware nur dann gewährleistet ist, wenn Runtime Firmware und SDR (Sensor Data Record, siehe Seite 378) demselben Firmware Release angehören.

10.1 Firmware des iRMC (Überblick)

Der iRMC verfügt über zwei separate EEPROMs (**E**lectrically **E**rasable **P**rogrammable **R**ead-**O**nly **M**emory), auf denen jeweils eine komplette Firmware gespeichert ist:

– EEPROM 1 (Low EEPROM)
– EEPROM 2 (High EEPROM)

Informationen zu Firmware und EEPROMs des iRMC erhalten Sie

– an der iRMC-Web-Oberfläche, Seite *iRMC Information* (siehe Seite 196) oder

– mithilfe der Flash-Tools (siehe Seite 391).

Aktiver und passiver EEPROM

Jeweils einer der beiden EEPROMs ist aktiv (running), während der andere inaktiv ist. Welcher EEPROM aktiv ist, wird über den so genannten Firmware Selector festgelegt (siehe Seite 379).

Struktur der iRMC-EEPROMs

Jeder EEPROM des iRMC ist in drei verschiedene Bereiche gegliedert:

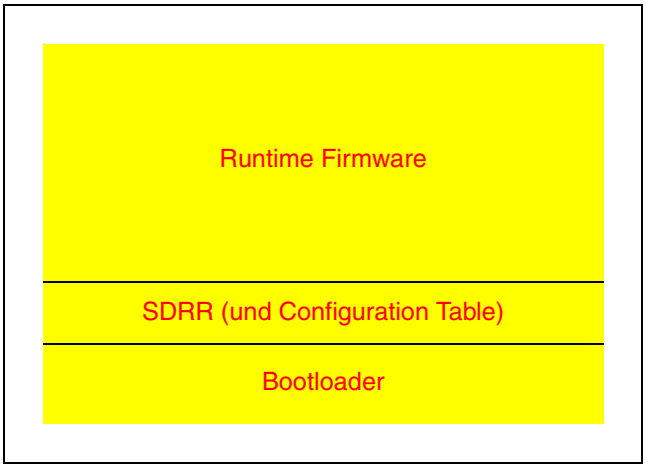


Bild 185: Struktur des iRMC-EEPROMs

– Runtime Firmware

  Die Runtime Firmware stellt den ablauffähigen Teil der Firmware des iRMC dar.

– SDRR (Sensor Data Record Repository)

  Das SDRR enthält die Sensor Data Records (SDR), in denen Sensor-Informationen des verwalteten Servers abgelegt sind. Außerdem dient das SDRR als Schnittstelle, über die Sie auf die SDRs zugreifen können.

– Bootloader

  Der Bootloader prüft die Firmware des zurzeit aktiven EEPROM. Bei fehlerhafter Firmware setzt der Bootloader den Firmware-Selektor auf den anderen EEPROM.

Für jeden dieser Bereiche können Sie einen Update durchführen.

Firmware Selector

Der Firmware Selector spezifiziert den EEPROM, dessen Firmware ausgeführt wird. Nach jedem Reset und Neustart des iRMC wird der Firmware Selector ausgewertet und es wird auf die entsprechende Firmware verzweigt.

Der Fimware Selector kann folgende Werte annehmen:

0 EEPROM mit der neuesten Firmware

1 EEPROM 1

2 EEPROM 2

3 EEPROM mit der ältesten Firmware

4 EEPROM mit der zuletzt aktualisierten Firmware

5 EEPROM mit der am längsten nicht mehr aktualisierten Firmware

Je nach verwendeter Update-Variante ist der Firmware Selector nach erfolgtem Update unterschiedlich gesetzt.

Mithilfe des Flash-Tools können Sie den Firmware Selector abfragen und explizit setzen (siehe Seite 391).

Firmware der einzelnen EEPROMs und EEPROM-Bereiche aktualisieren

Je nachdem, ob Sie den Firmware-Update online (siehe Seite 384) oder offline (siehe Seite 387) durchführen, können Sie nur die Firmware des inaktiven EEPROM oder auch des aktiven EEPROM aktualisieren:

– Bei einem Online-Firmware-Update können Sie nur die Firmware des inaktiven EEPROM aktualisieren.

– Bei einem Offline-Firmware-Update können Sie auch die Firmware des aktiven EEPROM aktualisieren.

10.2 USB Memory Stick erstellen

Den USB Memory Stick benötigen Sie **nicht**, wenn Sie die Firmware des iRMC via ServerView Update Manager, via ServerView Update Manager Express oder via ASP aktualisieren.

Gehen Sie wie folgt vor:

- Laden Sie die Firmware *Firmware Update for USB Stick* aus der Download-Section des Web-Servers von Fujitsu Technology Solutions in ein Verzeichnis auf Ihrem Rechner,

  oder

  legen Sie die aktuelle *PRIMERGY ServerView Suite DVD 1* in das DVD-ROM-Laufwerk Ihres Rechners ein.

  In Ihrem Download-Verzeichnis bzw. auf der DVD 1 finden Sie folgende Dateien bzw. folgendes ZIP-Archiv:

  - *FTS_<nnnnnnn>.exe*
  - *FTS_<nnnnnnn>.zip*

    Das Zip-Archiv enthält folgende Dateien:

    - *USBImage.exe*
    - *iRMC_<Firmware-Version>.IMA*

- Verbinden Sie den USB Memory Stick mit Ihrem Rechner.
- Starten Sie die Datei *FTS_<nnnnnnn>.exe* oder die Datei *USBImage.exe*.

  Je nachdem, welche Datei Sie aufrufen, wird eines der folgenden Fenster geöffnet:

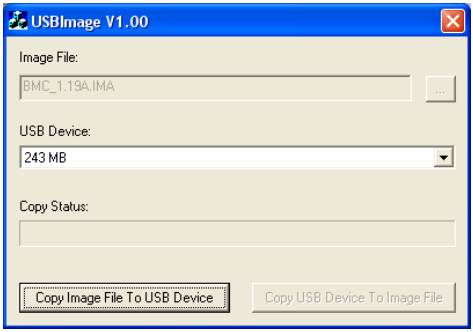


Bild 186: Image-Datei auf USB Memory Stick kopieren (FTS_<nnnnnnn>.exe)

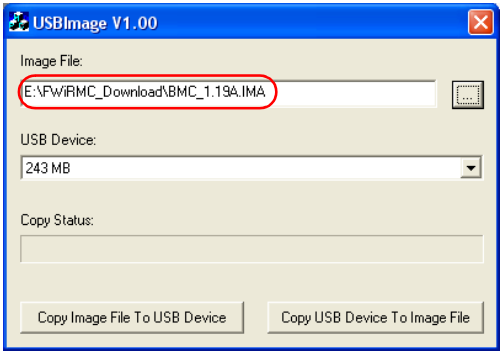


Bild 187: Image-Datei auf USB Memory Stick kopieren (USBImage.exe)

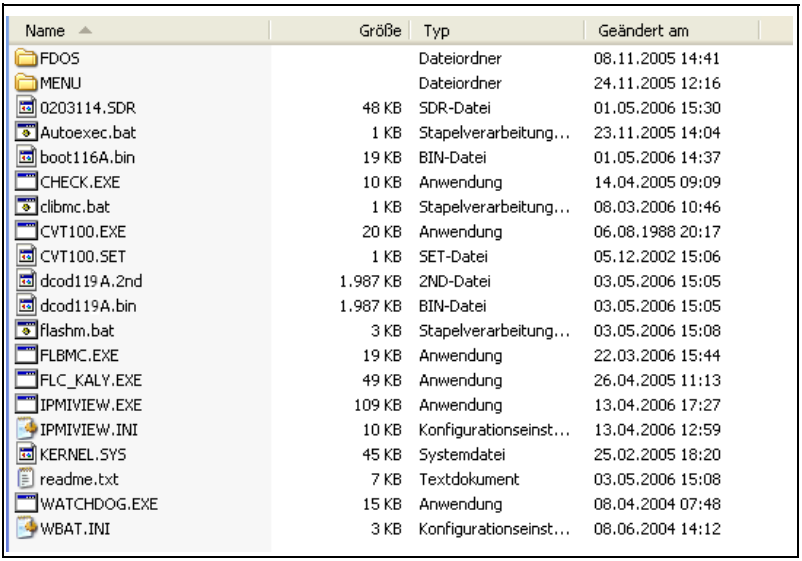
Wenn Sie *USBImag.exe* aufgerufen haben, müssen Sie unter *Image File:* die Datei *iRMC_<Firmware-Version>.IMA* explizit angeben.

- Klicken Sie auf *Copy Image File to USB Device*, um die Datei *iRMC_<Firmware-Version>.IMA* auf den USB Memory Stick zu kopieren und zu extrahieren.

ACHTUNG!

Durch diese Aktion wird der Inhalt des USB Memory Sticks überschrieben.

Nach Abschluss des Kopiervorgangs befinden sich Flash-Tools und Image-Dateien auf dem USB Memory Stick (siehe Bild 188 auf Seite 383).



Name	Größe	Typ	Geändert am
FDOS		Dateiordner	08.11.2005 14:41
MENU		Dateiordner	24.11.2005 12:16
0203114.SDR	48 KB	SDR-Datei	01.05.2006 15:30
Autoexec.bat	1 KB	Stapelverarbeitung...	23.11.2005 14:04
boot116A.bin	19 KB	BIN-Datei	01.05.2006 14:37
CHECK.EXE	10 KB	Anwendung	14.04.2005 09:09
clibmc.bat	1 KB	Stapelverarbeitung...	08.03.2006 10:46
CVT100.EXE	20 KB	Anwendung	06.08.1988 20:17
CVT100.SET	1 KB	SET-Datei	05.12.2002 15:06
dcod119A.2nd	1.987 KB	2ND-Datei	03.05.2006 15:05
dcod119A.bin	1.987 KB	BIN-Datei	03.05.2006 15:05
flashm.bat	3 KB	Stapelverarbeitung...	03.05.2006 15:08
FLBMC.EXE	19 KB	Anwendung	22.03.2006 15:44
FLC_KALY.EXE	49 KB	Anwendung	26.04.2005 11:13
IPMIVIEW.EXE	109 KB	Anwendung	13.04.2006 17:27
IPMIVIEW.INI	10 KB	Konfigurationseinst...	13.04.2006 12:59
KERNEL.SYS	45 KB	Systemdatei	25.02.2005 18:20
readme.txt	7 KB	Textdokument	03.05.2006 15:08
WATCHDOG.EXE	15 KB	Anwendung	08.04.2004 07:48
WBAT.INI	3 KB	Konfigurationseinst...	08.06.2004 14:12

Bild 188: Image-Dateien und Flash-Tools auf dem USB Memory Stick.

10.3 Online-Update

Bei einem Online-Update aktualisieren Sie die Firmware des iRMC bei laufendem Betriebssystem (Windows oder Linux) des verwalteten Servers.

Da während eines Online-Updates die Firmware des aktiven EEPROM weiter ausgeführt wird, können Sie beim Online-Update nur die Firmware des zum Update-Zeitpunkt inaktiven EEPROM aktualisieren.

Aus Gründen der Ausfallsicherheit ist es nicht möglich, einen Online-Firmware-Update für den Bootloader im EEPROM 1 (Low EEPROM) des iRMC durchzuführen.

Für den Online-Update der Firmware stehen Ihnen folgende Möglichkeiten zur Verfügung:

– Online-Update mit dem ServerView Update Manager

– Online-Update mit dem ServerView Update Manager Express oder via ASP

– Online-Update mithilfe der Betriebssystem-Flash-Tools.

10.3.1 Online-Update via ServerView Update Manager

Mithilfe des ServerView Update Managers (im Folgenden kurz Update Manager) können Sie den Update der iRMC-Firmware über eine grafische Benutzeroberfläche (Windows) oder über ein Command Line Interface (Windows und Linux) starten. Der Update Manager greift auf die Update-Daten über ein Update Manager-Dateiverzeichnis (Update-Repository) auf der *PRIMERGY ServerView Suite DVD 1* oder dem Management-Server zu. Das Update-Repository auf dem Management-Server aktualisieren Sie mittels Download-Manager oder manuellem Download aus der Download-Section des Web-Servers von Fujitsu Technology Solutions.

Näheres zum Firmware-Update mit dem Update Manager finden Sie im Handbuch „ServerView Update Manager“.

10.3.2 Online-Update via ServerView Update Manager Express oder ASP

Unter Windows- und Linux-Betriebssystemen können Sie die iRMC-Firmware wahlweise auch mithilfe der grafischen Benutzeroberfläche des ServerView Update Manager Express aktualisieren oder Sie verwenden die ASP (Autonomous Support Package)-Kommandoschnittstelle.

Unter Windows können Sie ein ASP außerdem im Windows-Explorer per Doppelklick auf die entsprechende ASP-*.*exe*-Datei starten.

Näheres zum Firmware-Update via ServerView Update Manager Express und ASP finden Sie im Handbuch „ServerView Update Manager Express“.

10.3.3 Online-Update mit den Betriebssystem-Flash-Tools

Ein Online-Update mithilfe der Betriebssystem-Flash-Tools wird nur als Recovery Flash durchgeführt, d.h. es erfolgt keine Versionsprüfung.

Abhängig vom eingesetzten Betriebssystem verwenden Sie eines der Flash-Tools WinFLBMC, RedhatFLBMC oder SuseFLBMC:

Windows:	WinFLBMC
Red Hat Linux:	RedhatFLBMC
Suse Linux:	SuseFLBMC

Die Flash-Tools rufen Sie in der Windows-Eingabeaufforderung (WinFLBMC) bzw. am Linux-CLI (RedhatFLBMC, SuseFLBMC) auf.

Syntax und Operanden der Flash-Tools sind beschrieben im Abschnitt „Flash-Tools“ auf Seite 391.

Voraussetzungen

– Die Flash-Tools sowie die Dateien für den Fimware-Update müssen im Dateisystem des verwalteten Servers vorhanden sein.

– Unter Windows und Linux: Die ServierView-Agenten müssen auf dem verwalteten Server gestartet sein.

Gehen Sie wie folgt vor:

Nachfolgend ist der Online-Update unter Verwendung eines USB Memory Sticks beschrieben (siehe Abschnitt „USB Memory Stick erstellen“ auf Seite 381).

- Verbinden Sie den USB Memory Stick mit dem verwalteten Server.
- Wechseln Sie in der Windows-Eingabeaufforderung oder im Command Line Interface (CLI) von Linux zum Laufwerk des USB Memory Sticks.
- Setzen Sie den Firmware Selector auf den Wert 4, indem Sie das Flash-Tool mit dem Parameter */s 4* aufrufen.

  Z. B. geben Sie in der Windows-Eingabeaufforderung an:

  ```
  WinFLBMC /s 4
  ```

- Starten Sie den Update der Firmware und der SDR-Daten, indem Sie das Flash-Tool mit den entsprechenden Update-Dateien aufrufen.

  Z. B. geben Sie in der Windows-Eingabeaufforderung an:

  ```
  WinFLBMC dcod<firmware-version>.bin <nnnnnnn>.sdr /p
  ```

  Während des Firmware-Updates werden Sie an der Konsole über den Verlauf des Update-Vorgangs informiert. Im Fehlerfall wird der Update-Vorgang abgebrochen und ein entsprechender Returncode gemeldet (siehe Seite 393).

- Starten Sie den verwalteten Server neu. Der EEPROM mit der aktualisierten Firmware wird dadurch automatisch aktiviert.

10.4 Offline-Update

Beim Offline-Update aktualisieren Sie die iRMC-Firmware aus einer DOS-Umgebung heraus. In diesem Fall können Sie die neben der Firmware des inaktiven EEPROM auch die Firmware des zurzeit aktiven EEPROM aktualisieren.

Während des Offline-Updates wird die aktive Firmware beendet und anschließend automatisch neu gestartet.

Für den Offline-Update der Firmware stehen Ihnen folgende Möglichkeiten zur Verfügung:

– Offline-Update mit dem ServerView Update Manager

– Offline-Update über das Menü der FlashDisk

– Offline-Update mithilfe des Flash-Tools flbmc

Beim Offline-Update können Sie den Firmware-Update auch für den Bootloader des Low EEPROM des iRMC durchführen.

10.4.1 Offline-Update via ServerView Update Manager

Mithilfe des ServerView Update Managers können Sie den Update der iRMC-Firmware über eine grafische Benutzeroberfläche (Windows) über ein Command Line Interface (Windows und Linux) starten. Der Update Manager greift auf die Update-Daten über ein Update Manager-Dateiverzeichnis (Update-Repository) auf der *PRIMERGY ServerView Suite DVD 1* oder dem Management-Server zu. Das Update-Repository auf dem Management-Server aktualisieren Sie mittels Download-Manager oder manuellem Download aus der Download-Section des Web-Servers von Fujitsu Technology Solutions.

Näheres zum Firmware-Update mithilfe des Update Managers finden Sie im Handbuch „ServerView Update Manager“.

10.4.2 Offline-Update über das Menü der FlashDisk

Für den Offline-Update über das Menü der FlashDisk benötigen Sie einen boot-fähigen USB Memory Stick (siehe Abschnitt „USB Memory Stick erstellen“ auf Seite 381).

Gehen Sie wie folgt vor:

- Verbinden Sie den USB Memory Stick mit dem verwalteten Server.
- Booten Sie vom USB Memory Stick.

Nach Abschluss des Bootvorgangs werden die Daten des USB Memory Sticks automatisch in eine RAM Disk kopiert. Anschließend wird die Datei *autoexec.bat* automatisch gestartet.

Das FlashDisk-Menü wird geöffnet:

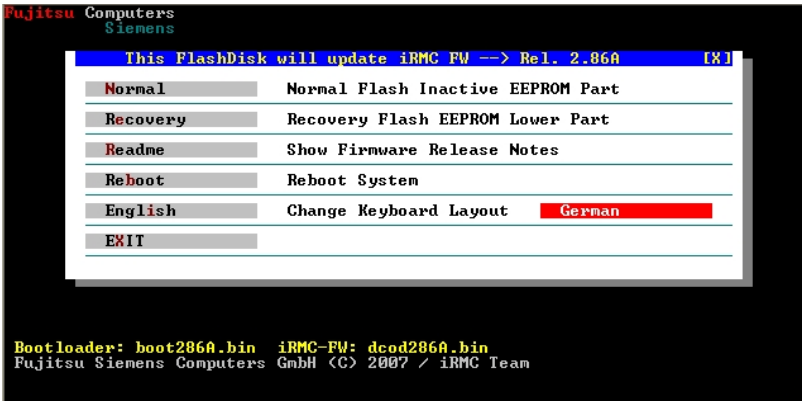


Bild 189: Menü der FlashDisk

Normal

Es wird ein *Normal Flash* durchgeführt.

Bei einem Normal Flash werden die Bereiche des aktiven EEPROM auf Aktualität überprüft. Ist ein Bereich nicht aktuell, so wird der korrespondierende Bereich auf dem inaktiven EEPROM aktualisiert, sofern er nicht bereits aktuell ist.

Recovery

Es wird ein *Recovery Flash* durchgeführt.

Bei einem Recovery Flash wird der Flash ohne Versionsprüfung für alle drei Bereiche des EEPROM durchgeführt. Der Firmware-Update wird für den EEPROM 1 durchgeführt. Ein Firmware-Downgrade ist nur via Recovery Flash möglich.

Readme

Die Readme-Datei mit wird angezeigt.

Reboot

Es wird ein Warmstart des iRMC durchgeführt.

English / *German*

Tastatur-Layout festlegen. Standardmäßig ist *German* eingestellt.

- Starten Sie die gewünschte Update-Variante durch Anklicken der entsprechenden Schaltfläche.

  Während des Firmware-Updates werden Sie an der Konsole über den Verlauf des Update-Vorgangs informiert. Im Fehlerfall wird der Update-Vorgang abgebrochen. Ein entsprechender Returncode wird gemeldet (siehe Seite 393).

- Klicken Sie nach Abschluss des Update-Vorgangs auf *Exit*, um das FlashDisk-Menü zu verlassen.

- Trennen Sie den USB Memory Stick vom verwalteten Server.

- Starten Sie den verwalteten Server neu (z.B. mit Ctrl + Alt + Del).

10.4.3 Offline-Update mit dem Flash-Tool flbmc

Einen Offline-Update können Sie auch starten, indem Sie im DOS-Eingabefenster das Flash-Tool flbmc mit den entsprechenden Parametern aufrufen. Syntax und Operanden des Flash-Tools sind beschrieben im Abschnitt „Flash-Tools“ auf Seite 391.

Ein Offline-Update mithilfe des Flash-Tools flbmc kann nur als Recovery Flash durchgeführt werden, d.h. es erfolgt keine Versionsprüfung.

Per Offline-Update mit dem Flash-Tool flbmc können Sie den Recovery Flash optional auch für den EEPROM 2 durchführen.

10.5 Emergency Flash

Wenn die Firmware des iRMC nicht mehr ausgeführt werden kann, z. B. weil die SDRs nicht mit dem System kompatibel sind, können Sie über den Emergency Mode die Firmware wieder zum Laufen bringen. Im Emergency Mode verzweigt das System automatisch zum Bootloader und ist dann bereit für den Firmware-Update.

Um den verwalteten Server in den Emergency Mode zu versetzen und anschließend die Firmware des iRMC zu aktualisieren, verfahren Sie wie folgt:

- ► Ziehen Sie den Netzstecker.
- ► Stecken Sie den Stecker bei gedrückter Identify-Taste wieder in die Steckdose.

  Der verwaltete Server befindet sich nun im Emergency Mode.
- ► Booten Sie den Server nach DOS und aktualisieren Sie die Firmware des iRMC per Recovery Flash (siehe Abschnitt „Offline-Update“ auf Seite 387).

  Wenn die Firmware nicht aktiv ist, startet der Bootvorgang mit einer zeitlichen Verzögerung von bis zu 2 Minuten. Die Fehlermeldung „iRMC Controller Error“, die das BIOS während dieser Zeit ausgibt, können Sie ignorieren.

10.6 Flash-Tools

Die Tools WinFLBMC, RedhatFLBMC und SuseFLBMC unterscheiden von flbmc nur im Tool-Namen sowie in der Umgebung, in der sie aufgerufen werden. Die nachfolgende Beschreibung gilt somit auch für die Tools WinFLBMC, RedhatFLBMC und SuseFLBMC. Anstelle von „flbmc“ ist dabei jeweils „WinFLBMC“, „RedhatFLBMC“ bzw. SuseFLBMC anzugeben.

Syntax

```
flbmc {/v|/o [/4]|/s[<Wert>]}

flbmc {<datei1> [<datei2>] [<datei3>]
      [/n /l[<logdatei>] /d /e /4 /p]}

flbmc {/h|/?}
```

Optionen

/v Aktuellen Versionsstand des Kommandos anzeigen.

/o Aktuellen Versionsstand der Firmware von EEPROM 1 anzeigen.

/o /4 Aktuellen Versionsstand der Firmware von EEPROM 2 anzeigen.

/s Aktuellen Wert des Firmware-Selektors anzeigen.

/s <Wert>

Wert des Firmware-Selektors setzen. Mit dieser Option legen Sie fest, aus welchem EEPROM die Firmware nach einem Firmware-Reset gestartet wird.

- 0 Selektor auf den EEPROM mit der neuesten Firmware setzen.
- 1 Selektor auf den EEPROM 1 setzen.
- 2 Selektor auf den EEPROM 2 setzen.
- 3 Selektor auf den EEPROM mit der ältesten Firmware setzen.
- 4 Selektor auf den EEPROM mit der zuletzt aktualisierten Firmware setzen.
- 5 Selektor auf den EEPROM mit der am längsten nicht mehr aktualisierten Firmware setzen.

<datei1> bis <datei3>

Mit der Angabe einer oder mehrerer Dateien legen Sie fest, welche Aktualisierung(en) vorgenommen werden soll(en). Folgende Dateien stehen zur Auswahl:

boot<FW-Version>.bin

Aktualisierung der Bootloader-Firmware.

dcod<FW-Version>.bin

Aktualisierung der Runtime-Firmware für EEPROM 1.

dcod<FW-Version>.2nd

Aktualisierung der Runtime-Firmware für EEPROM 2.

<SDR-Version>.SDR

Aktualisierung des SDR-Datensatzes.

dcod<FW-Version>.bin und *dcod<FW-Version>.2nd* dürfen nicht gleichzeitig im selben Aufruf des Flash-Tools angegeben werden.

Wenn Sie die Datei *dcod<FW-Version>.2nd* angeben, ist die Option */4* (siehe unten) nicht erforderlich, da durch das Suffix *.2nd* bereits der EEPROM 2 ausgewählt wird. Andernfalls müssen Sie für eine Aktualisierung des EEPROM 2 die Option */4* angeben.

/4 EEPROM 2 aktualisieren.

Das Kommando verhält sich bezüglich der Option */4* wie folgt:

- Wenn Sie */4* in Verbindung mit der *dcod*-Datei für den EEPROM 1 angeben, wird geprüft, ob im gleichen Verzeichnis eine identische Firmware-Version für den EEPROM 2 existiert. Ist dies der Fall, so wird die Firmware für den EEPROM 2 aktualisiert, andernfalls wird das Kommando mit einer Fehlermeldung und dem Rückgabewert 5 beendet.
- Wenn Sie */4* in Verbindung mit der *dcod*-Datei für den EEPROM 2 nicht angeben, wird geprüft, ob im gleichen Verzeichnis eine identische Firmware-Version für den EEPROM 1 existiert. Ist dies der Fall, so wird die Firmware für den EEPROM 1 aktualisiert, andernfalls wird das Kommando mit einer Fehlermeldung und dem Rückgabewert 5 beendet.

/l [<logdatei>]

Ausgabe von Fehlermeldungen in die angegebene Logdatei. Wenn Sie Logdatei angeben, erfolgt die Ausgabe in die Datei *flbmc.log*.

/n Keine Ausgabe auf der Konsole.
Diese Option übersteuert die Optionen */p* und */d*.

/p Fortschrittsanzeige des Aktualisierungsprozesses in Prozent.

/d Ausgabe zusätzlicher Debug-Informationen.

/e Emulationsmodus (nur für Debug-Zwecke).

/h und /?
Ausgabe von Hilfe-Informationen.

Rückgabewerte

0	Aktualisierung erfolgreich ausgeführt.
1	Unzulässige oder fehlende Optionen.
3	PROM-Typ nicht verfügbar.
4	Kommunikation mit iRMC nicht möglich.
5	Fehlerhaft Binärdatei.
8	Fehler beim Zugriff auf die Keyboard Control Style-Schnittstelle (KCS).
9	Zeitüberschreitung während der Kommunikation mit dem Ziel-EEPROM.
10	Kein Pufferspeicher zugewiesen.
12	Netzknoten belegt.
13	Zeitüberschreitung beim Löschen des EEPROM.
14	Zeitüberschreitung bei der Aktualisierung des EEPROM.
15	Fehler beim Löschen des EEPROM.
16	Fehler bei der Aktualisierung des EEPROM.

11 Remote-Installation des Betriebssystems via iRMC

Dieses Kapitel beschreibt, wie Sie mithilfe des ServerView Installation Managers (im Folgenden kurz Installation Manager) sowie mittels der iRMC-Features „Advanced Video Redirection (AVR)“ und „Remote Storage“ und „Advanced Video Redirection (AVR)“ vom Remote-Arbeitsplatz aus das Betriebssystem auf dem verwalteten Server installieren.

Im Einzelnen informiert das Kapitel über folgende Themen:

– Generelles Vorgehen bei der Remote-Installation eines Betriebssystems mithilfe von Remote Storage-Speichermedien.

– Verwalteten Server vom Remote-Arbeitsplatz aus über die PRIMERGY ServerView DVD 1 booten (Windows und Linux).

– Windows nach Konfiguration auf dem verwalteten Server vom Remote-Arbeitsplatz aus installieren.

– Linux nach Konfiguration auf dem verwalteten Server vom Remote-Arbeitsplatz aus installieren.

Die Beschreibung legt den Schwerpunkt auf das Handling der Remote Storage-Speichermedien. Kenntnisse der Funktionalität des Installation Managers werden vorausgesetzt (siehe Handbuch „PRIMERGY ServerView Suite - ServerView Installation Manager“).

Voraussetzungen für eine Remote-Installation des Betriebssystems via iRMC:

– Die LAN-Schnittstelle des iRMC muss konfiguriert sein (siehe Seite 38).

– Der License Key für die Nutzung der iRMC-Features „Advanced Video Redirection (AVR)“ und „Remote Storage“ muss installiert sein (siehe Seite 198).

– Die Text-Konsolumleitung muss deaktiviert sein (siehe Seite 281).

11.1 Betriebssystem via iRMC installieren - generelles Vorgehen

Die Remote-Installation des Betriebssystems via iRMC ist aus Sicht des Installation Managers eine lokale Konfiguration und Installation des Betriebssystems auf dem verwalteten Server, die Sie vom Remote-Arbeitsplatz aus über das AVR-Fenster mithilfe von Remote Storage-Speichermedien durchführen.

Im Einzelnen sind für eine Installation mittels Installation Manager folgende Schritte erforderlich:

1. Speichermedium (DVD 1 oder Installation Manager Boot-Image), von dem gebootet werden soll, als Remote Storage verbinden.
2. Verwalteten Server vom Remote-Arbeitsplatz aus über die DVD 1 oder Installation Manager Boot-Image booten und konfigurieren.
3. Betriebssystem via Installation Manager vom Remote-Arbeitsplatz aus auf dem verwalteten Server installieren.
4. Mauszeiger-Synchronisation im AVR-Fenster optimieren (nur unter Linux erforderlich).

Windows ohne Installation Manager mithilfe der Windows-Installations-CD/DVDs installieren

Die Remote-Installation von Windows via Remote Storage können Sie wahlweise mithilfe des Installation Managers oder ausschließlich mithilfe der Windows-Installations-CD/DVDs durchführen. Hinsichtlich des Handlings der Remote Storage-Speichermedien stimmen beide Verfahren überein.

Aus folgenden Gründen empfiehlt sich jedoch eine Windows-Installation mithilfe des Installation Managers:

– Der Installation Manager ermittelt selbstständig die erforderlichen Treiber und kopiert diese in das System.

– Während der Installation stehen Ihnen alle Installation Manager-Funktionen zur Verfügung. So können Sie z.B. das gesamte System inklusive der Einstellungen für das Server-Management konfigurieren.

– Die Installation ohne Installation Manager müssen Sie über die Tastatur steuern, da während des Installationsvorgangs der Mauszeiger nicht synchronisiert werden kann. Dagegen können Sie bei der Installation via Installation Manager die gesamte Konfiguration und Installation mithilfe der Maus abwickeln.

– Bei der Installation ohne Installation Manager müssen Sie alle erforderlichen Einstellungen für die Synchronisation des Mauszeigers nachträglich „von Hand“ durchführen.

– Die Installation via Installation Manager dauert nicht wesentlich länger als die Installation mithilfe der Betriebssystem-CD/DVDs.

Linux ohne Installation Manager mithilfe der Linux-Installations-CDs installieren

Wenn Sie die vom System benötigten Treiber kennen, können Sie die Linux-Installation auch durch Booten von der Linux-Installations CD/DVD starten.

Falls die Installation eine Treiber-Integration von der Floppy-Disk erfordert, müssen Sie vor Beginn der Installation jeweils eine Remote Storage-Verbindung zu folgenden Speichermedien einrichten:

– Speichermedium (CD-ROM/DVD-ROM oder ISO Image), von dem aus gebootet werden soll, sowie

– ggf. Speichermedium für die Treiber-Installation.

11.2 Speichermedium als Remote Storage verbinden

Remote Storage stellt dem verwalteten Server ein „virtuelles“ Laufwerk zur Verfügung, das sich an anderer Stelle im Netz befindet.

Die Source für das virtuelle Laufwerk kann sein:

– Physisches Laufwerk oder Image-File am Remote-Arbeitsplatz. Das Image-File kann außerdem auf einem Netzlaufwerk liegen (mit Laufwerksbuchstaben, z.B. „D:“ für Laufwerk D).

– Image-File, das mithilfe eines Remote Storage Servers zentral im Netz bereitgestellt wird.

Parallele Remote Storage-Verbindungen:

Zur selben Zeit möglich sind entweder

– **maximal zwei** Remote Storage-Verbindungen zu virtuellen Laufwerken am Remote-Arbeitsplatz (bei Verbindungsaufbau via AVR Java-Applet)

oder

– **eine** Remote Storage-Verbindung zu einem Remote Storage Server.

Remote Storage-Verbindungen via Applet und Remote Storage Server sind nicht gleichzeitig möglich.

Mithilfe der Seite *Remote Storage* der iRMC-Web-Oberfläche können Sie Sie sich über den Status der aktuellen Remote Storage-Verbindungen informieren (siehe Seite 300).

Ausführliche Informationen zu Remote Storage finden Sie im Kapitel „Remote Storage“ auf Seite 159.

Speichermedium am Remote-Arbeitsplatz als Remote Storage verbinden

Für das Booten von einem virtuellen Laufwerk, das sich am Remote-Arbeitsplatz befindet, werden folgende Gerätetypen unterstützt:

> **i** Das Booten von einem USB Memory Stick wird nur dann unterstützt, wenn der USB Memory Stick als Floppy Disk emuliert ist.

- Floppy-Disk (physisches Speichermedium))
- CD-ROM (physisches Speichermedium)
- DVD-ROM (physisches Speichermedium)
- ISO Image (Image-File)

Zum Herstellen der Remote Storage-Verbindung gehen Sie am Remote-Arbeitsplatz wie folgt vor:

- ► Melden Sie sich mit Remote Storage Enabled-Berechtigung an der iRMC-Web-Oberfläche an (siehe Seite 182).
- ► Öffnen Sie die Seite *Advanced Video Redirection* und starten Sie die AVR (siehe Seite 292).
- ► Starten Sie im AVR-Fenster „Remote Storage“ (siehe Seite 161).

► Stellen Sie die Speichermedien für Remote Storage bereit (siehe Seite 163):

– Bei Installation via Installation Manager:

PRIMERGY ServerView Suite DVD 1 oder Installation Manager-Boot-Image sowie optional einen formatierten USB Memory Stick als Status-Backup-Medium.

– Bei Installation via Installations-CD/DVD des Herstellers: Windows oder Linux Installations-CD/DVD und optionale Treiber.

Es wird empfohlen, die PRIMERGY ServerView Suite DVD 1 bzw. die Betriebssystem-Installations-CD/DVD als Image-File (ISO Image) in einem Verzeichnis abzulegen und von dort als Remote Storage zu verbinden oder via Remote Storage Server zur Verfügung zu stellen.

Die bereitgestellten Speichermedien werden in der Dialogbox *Storage Devices* angezeigt:

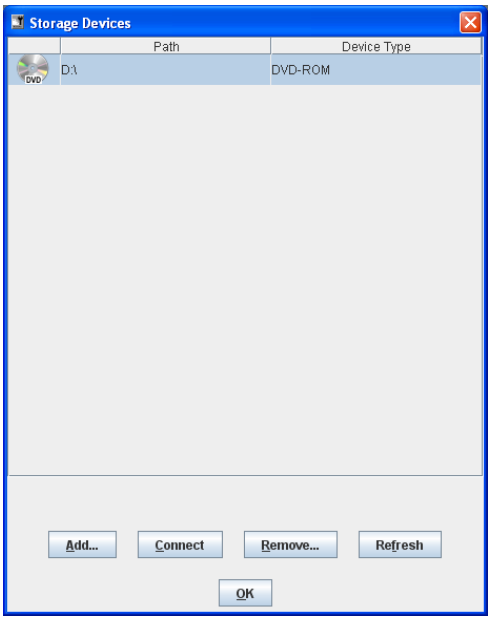


Bild 190: Dialogbox Storage Devices: PRIMERGY ServerView Suite DVD 1

► Klicken Sie auf *Connect*, um das DVD-ROM-Laufwerk (DVD 1) oder das Installation Manager Boot-Image als Remote Storage zu verbinden.

Vom Remote Storage Server bereitgestelltes ISO Image (Image-File) als Remote Storage verbinden

Ein via Remote Storage Server bereitgestelltes Image-File können Sie zum Booten von einem Installation Manager Boot-Image verwenden.

Die Nutzung eines via Remote Storage Server bereitgestellten virtuellen Laufwerks setzt voraus, dass der Remote Storage Server installiert und gestartet ist (siehe Abschnitt „Remote Storage via Remote Storage Server bereitstellen“ auf Seite 169).

Zum Erstellen der Verbindung zu Remote Storage Server gehen Sie am Remote-Arbeitsplatz wie folgt vor:

- Melden Sie sich mit *Remote Storage Enabled*-Berechtigung an der iRMC-Web-Oberfläche an (siehe Seite 182).
- Wählen Sie die Seite *Remote Storage*.
- Stellen Sie die Verbindung zum Remote Storage Server her (siehe Seite 301).

11.3 Verwalteten Server von der PRIMERGY ServerView Suite DVD 1 booten und via Installation Manager konfigurieren

Verwalteten Server von der PRIMERGY ServerView Suite DVD 1 booten

Gehen Sie am Remote-Arbeitsplatz wie folgt vor:

- Schalten Sie über die iRMC-Web-Oberfläche den verwalteten Server ein oder starten Sie den Server neu (siehe Seite 214).

  Den Bootvorgang können Sie im AVR-Fenster verfolgen. Während der BIOS POST-Phase des verwalteten Servers werden Remote Storage-Speichermedien als USB Geräte angezeigt.
- Drücken Sie während des Boot des Servers die Taste F2.
- Rufen Sie im BIOS-Setup das Menü für die Festlegung der Boot-Sequenz auf:

  Main – Boot Sequence.
- Legen Sie die Boot-Sequenz gemäß Bild 191 fest.

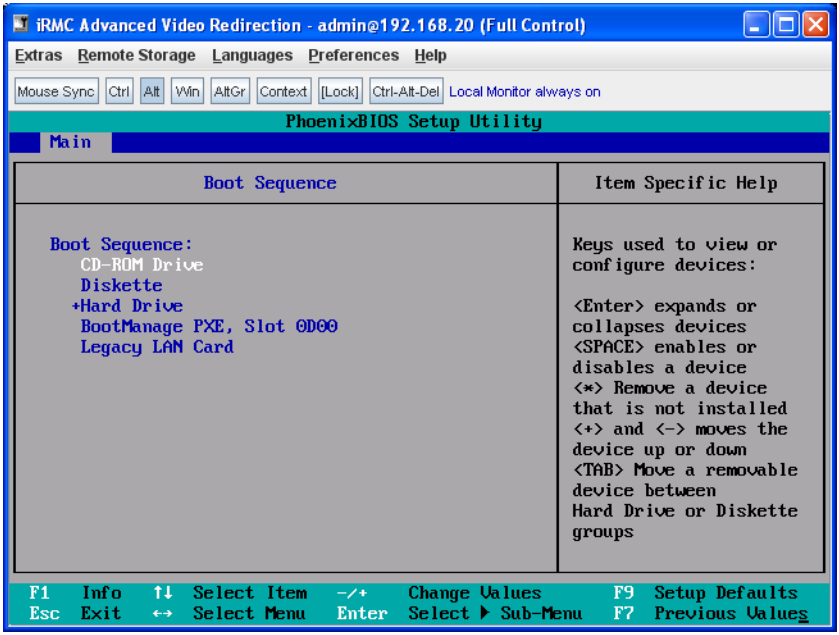

iRMC Advanced Video Redirection - admin@192.168.20 (Full Control)
Extras Remote Storage Languages Preferences Help
Mouse Sync Ctrl Alt Win AltGr Context [Lock] Ctrl-Alt-Del Local Monitor always on
PhoenixBIOS Setup Utility
Main
Boot Sequence
Item Specific Help
Boot Sequence:
CD-ROM Drive
Diskette
+Hard Drive
BootManage PXE, Slot 0D00
Legacy LAN Card
Keys used to view or configure devices:
<Enter> expands or collapses devices
<SPACE> enables or disables a device
<*> Remove a device that is not installed
<+> and <-> moves the device up or down
<TAB> Move a removable device between Hard Drive or Diskette groups
F1 Info ↑↓ Select Item -/+ Change Values F9 Setup Defaults
Esc Exit ↔ Select Menu Enter Select ▶ Sub-Menu F7 Previous Values

Bild 191: Menü Boot Sequence im BIOS-Setup

► Sichern Sie Ihre Einstellungen und verlassen Sie das BIOS-Setup.

Danach bootet der verwaltete Server von der als Remote Storage verbundenen PRIMERGY ServerView Suite DVD 1.

Falls das System nicht vom Remote Storage-Speichermedium (PRIMERGY ServerView Suite DVD 1 oder Installation Manager Boot-Image) bootet:

► Prüfen Sie, ob das Speichermedium während der BIOS POST-Phase angezeigt wird, und verbinden Sie erforderlichenfalls das Speichermedium als Remote Storage.

► Stellen Sie die korrekte Boot-Reihenfolge sicher.

Das Booten von der PRIMERGY ServerView Suite DVD 1 via Remote Storage-Speichermedium dauert ca. 5 Minuten.

Während des Bootvorgangs wird das folgende Fenster angezeigt (siehe Bild 192 auf Seite 404):

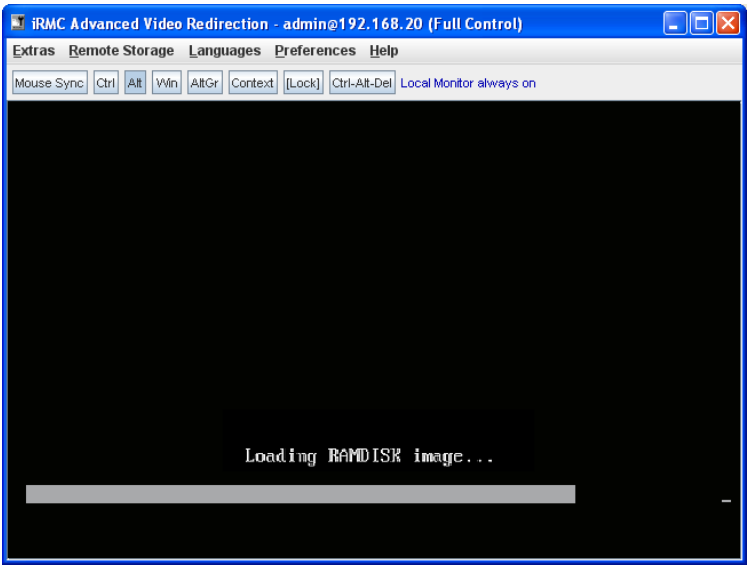
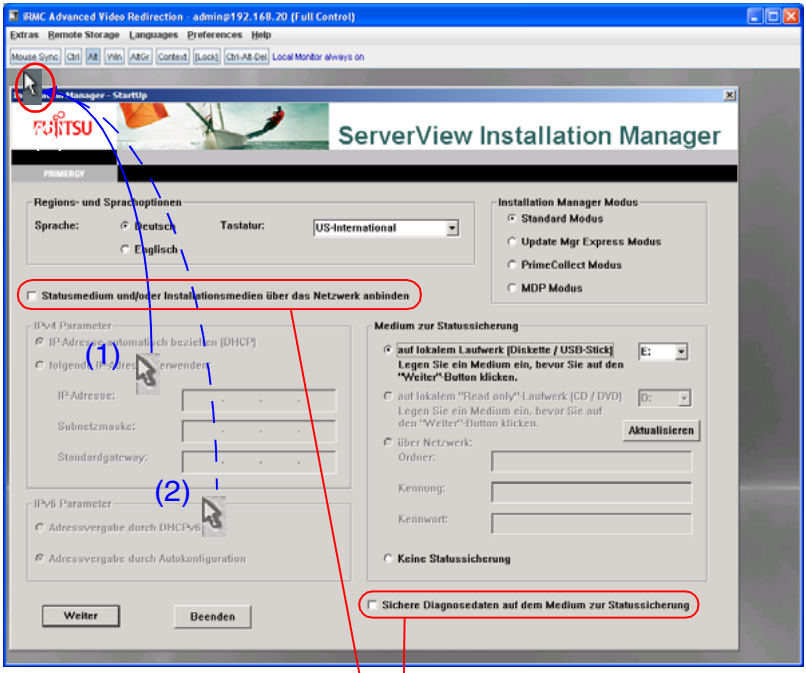

iRMC Advanced Video Redirection - admin@192.168.20 (Full Control)
Extras Remote Storage Languages Preferences Help
Mouse Sync Ctrl Alt Win AltGr Context [Lock] Ctrl-Alt-Del Local Monitor always on
Loading RAMDISK image...

Bild 192: Verwalteter Server wird von der PRIMERGY ServerView Suite DVD 1 gebootet.

Installation Manager Modus wählen und Medium zur Statussicherung festlegen

Nach Abschluss des Bootvorgangs wird das Startfenster des Installation Managers angezeigt, in dem Sie ein Medium für den Statussicherungsbereich (Status-Backup-Medium) auswählen können (siehe Bild 193 auf Seite 405).

Bevor Sie mit der Installation des Betriebssystems beginnen, sollten Sie im AVR-Fenster am Remote-Arbeitsplatz den lokalen Mauszeiger und den Mauszeiger des verwalteten Servers synchronisieren (siehe Bild 193 auf Seite 405). Näheres zur Synchronisation der Mauszeiger im AVR-Fenster finden Sie im Abschnitt „Mauszeiger synchronisieren“ auf Seite 144.



Mouse Sync-Taste drücken

oder

Optionen für Statussicherung

(1) Lokalen Mauszeiger in die linke obere Ecke ziehen.

(2) Mauszeiger des Servers folgt automatisch.

(3) Die Mauszeiger sind synchronisiert, wenn sie sich vollständig überlappen und im AVR-Fenster als **ein** Mauszeiger dargestellt werden.

Bild 193: Installation Manager: Status-Backup-Medium auswählen

- Wählen Sie unter *Installation Manager Modus* den *Standard Modus*.
- Legen Sie fest, ob die Konfigurationsdaten auf einem lokalen Wechseldatenträger oder einem Netzwerkmedium gespeichert werden sollen:

  Beachten Sie: Wenn Sie keine Option zur Statussicherung wählen, gehen sämtliche Konfigurationsdaten bei einem Reboot verloren.

Medium zur Statussicherung

Das Backup-Medium darf nicht schreibgeschützt sein.

Ein USB-Stick muss bereits beim Systemstart am USB-Port angeschlossen sein. Falls dies versäumt wurde und Sie die Konfigurationsdatei abspeichern wollen:

Schließen Sie den USB-Stick jetzt an und starten Sie einen Reboot von der PRIMERGY ServerView Suite DVD 1.

- Wählen Sie die Option *auf lokalem Laufwerk (Diskette / USB Stick)*.
- Wählen Sie im Auswahlfeld rechts von der Option das entsprechende Laufwerk aus.

  Nähere Informationen zur Erzeugung von Installation Manager-Statusdisketten erhalten Sie im Handbuch „ServerView Installation Manager“.

Statusmedium und/oder Installationsmedien über das Netzwerk anbinden

- Treffen Sie zu diesem Zweck die erforderlichen Freigaben.

  Wenn Sie ein Medium mit einer vorbereiteten Konfigurationsdatei und/oder ein Installationsmedium via Netz bereitstellen, müssen Sie diese Option wählen. Für die aktuelle Installation Manager-Sitzung können Sie, abhängig von Ihrer Infrastruktur, entweder eine temporäre IP-Adresse via DHCP beziehen oder manuell eine IPv4- oder IPv6-Adresse konfigurieren.

- Starten Sie den Installation Manager durch Klicken auf *Weiter*.

Lokales Deployment starten

Nach dem Start des Installation Managers wird das Begrüßungsfenster angezeigt:

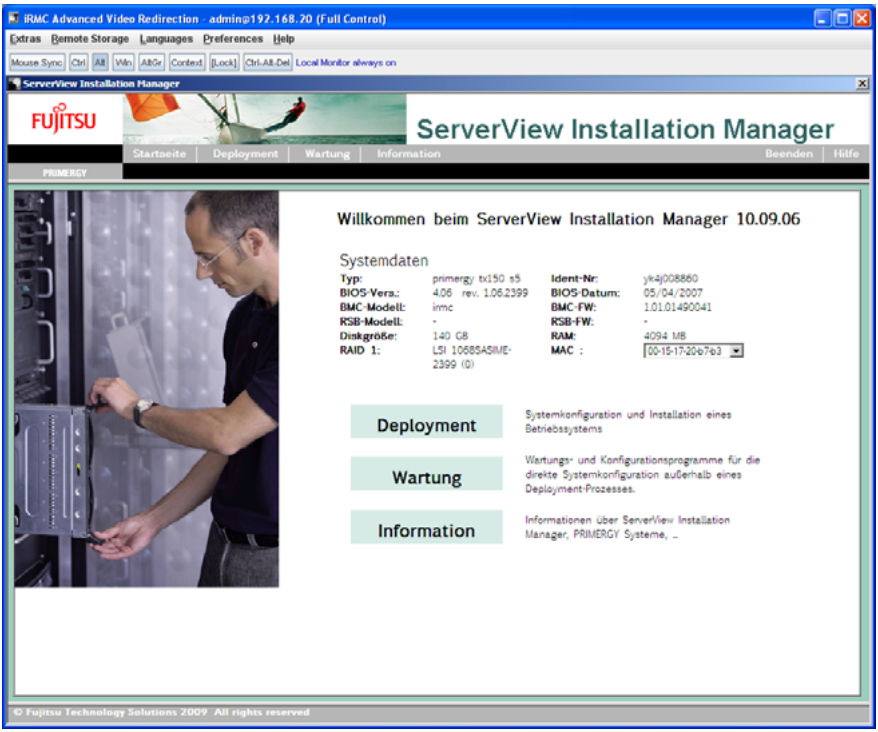

iRMC Advanced Video Redirection - admin@192.168.20 (Full Control)
Extras Remote Storage Languages Preferences Help
Mouse Sync Ctrl Alt Win AltGr Context [Lock] Ctrl-Alt-Del Local Monitor always on
ServerView Installation Manager
FUJITSU
ServerView Installation Manager
Startseite Deployment Wartung Information Beenden Hilfe
PRIMERGY
Willkommen beim ServerView Installation Manager 10.09.06
Systemdaten
Typ: primergy tx150 s5
BIOS-Vers.: 4.06 rev. 1.06.2399
BMC-Modell: irmc
RSB-Modell: -
Diskgröße: 140 GB
RAID 1: LSI 1068SASIME-2399 (0)
Ident-Nr: yk4j008860
BIOS-Datum: 05/04/2007
BMC-FW: 1.01.01490041
RSB-FW: -
RAM: 4094 MB
MAC : 00-15-17-20-b7-e3
Deployment
Systemkonfiguration und Installation eines Betriebssystems
Wartung
Wartungs- und Konfigurationsprogramme für die direkte Systemkonfiguration außerhalb eines Deployment-Prozesses.
Information
Informationen über ServerView Installation Manager, PRIMERGY Systeme, ...
© Fujitsu Technology Solutions 2009 All rights reserved

Bild 194: Installation Manager - Begrüßungsfenster

► Klicken Sie auf *Deployment*, um die Vorbereitung der lokalen Installation (Deployment) zu starten.

Zur Vorbereitung der Installation werden Sie von den Wizards des Installation Managers durch eine Folge von Konfigurationsschritte geführt, in denen Sie die Vorgaben für die Konfiguration des Systems sowie für die anschließende bedienerlose Betriebssystem-Installation zusammenzustellen.

Konfigurieren Sie als Installationsquelle das lokale CD-ROM/DVD-ROM-Laufwerk des verwalteten Servers. Dann können Sie die Windows Installations-CD/DVD auch über das CD-ROM/DVD-ROM-Laufwerk des Remote-Arbeitsplatzes bereitstellen, wenn Sie dieses als Remote Storage mit dem verwalteten Server verbinden (siehe Abschnitt „Windows nach Konfiguration auf dem verwalteten Server installieren“ auf Seite 409).

Nach Abschluss der Konfiguration mit dem Installation Manager wird der Dialog *Installationsparameter* für die Windows-Installation (siehe Seite 409) bzw. für die Linux-Installation (siehe Seite 413) angezeigt, über den Sie den installationsprozess starten können.

11.4 Betriebssystem nach Konfiguration auf dem verwalteten Server installieren

Im Anschluss an die Konfiguration installieren Sie das Betriebssystem auf dem verwalteten Server.

11.4.1 Windows nach Konfiguration auf dem verwalteten Server installieren

Nach Abschluss der Konfiguration zeigt der Installation Manager folgenden Dialog an:

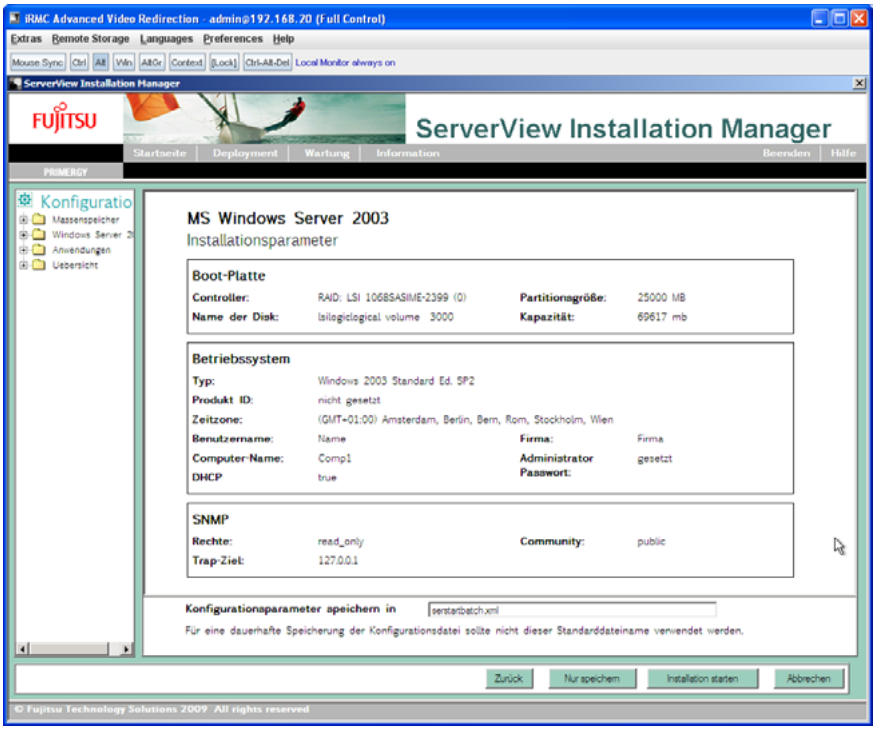


Bild 195: Installation Manager - Installation starten

Wenn Sie als Installationsquelle das lokale CD-ROM/DVD-ROM-Laufwerk des verwalteten Servers konfiguriert haben, gehen Sie am Remote-Arbeitsplatz wie folgt vor:

- Trennen Sie Ihre zurzeit aktiven Remote Storage-Verbindungen. Näheres zum Trennen von Remote Storage-Verbindungen finden Sie auf Seite 167.
- Entfernen Sie die PRIMERGY ServerView Suite DVD 1 aus dem DVD-ROM-Laufwerk am Remote-Arbeitsplatz.
- Legen Sie die Windows Installations-CD/DVD in dieses DVD-ROM-Laufwerk ein.

  Schließen Sie die Anwendung, falls *autostart* aktiviert ist.

- Verbinden Sie das CD-ROM/DVD-ROM-Laufwerk, das die Windows-Installations-CD/DVD enthält, als Remote Storage (siehe Seite 165).
- Klicken Sie auf *Installation starten*.

  Alle Installationsdateien werden auf den verwalteten Server kopiert.

  In einem Bestätigungsdialog informiert Sie der Installation Manager über den Abschluss des Kopiervorgangs und fordert Sie auf, vor dem automatischen Neustart des verwalteten Servers alle Speichermedien aus den Wechsellaufwerken zu entfernen.

  Insbesondere müssen Sie vor dem Neustart des Systems auch alle aktiven Remote Storage-Verbindungen trennen.

- Trennen Sie vor dem Neustart des Systems die aktuellen Remote Storage-Verbindungen.

  Verfahren Sie hierfür wie folgt:

  - Starten Sie Remote Storage (siehe Seite 161).

    Es wird die Dialogbox *Storage Devices* mit den aktuell verbundenen Speichermedien und dem Hinweis auf „Safe Remove“ angezeigt (siehe Bild 196 auf Seite 411).

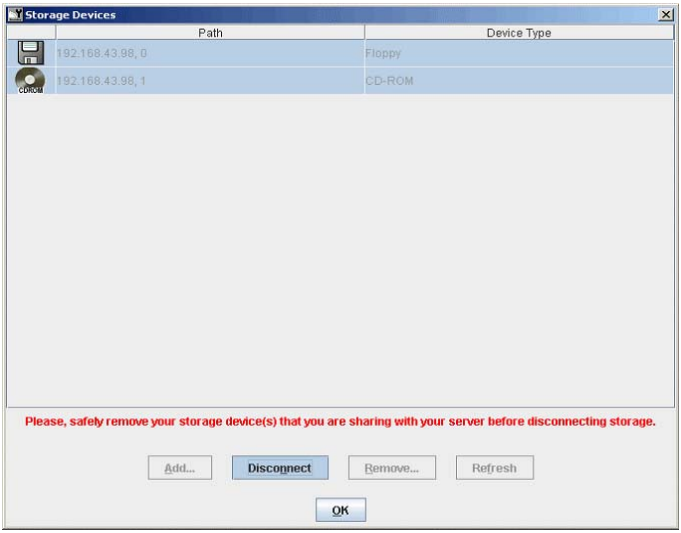


Bild 196: Dialogbox Storage Devices: Remote Storage-Verbindungen trennen

- ► Führen Sie einen „Safe Remove“ für die angezeigten Speichermedien durch, d.h. stellen Sie sicher, dass keine Anwendungen/Programme mehr auf die Speichermedien zugreifen.
- ► Klicken Sie auf *Disconnect...*, um alle Remote Storage-Verbindungen zu trennen.

► Klicken Sie im Bestätigungsdialog r auf *Ok*, um den verwalteten Server neu zu starten.

Nach dem Neustart des verwalteten Servers können Sie komplette Installation mithilfe der AVR überwachen (siehe Bild 197 auf Seite 412).

iRMC Advanced Video Redirection - admin@172.25.92.155 (Full Control)
Extras Remote Storage Languages Preferences Help
Mouse Sync Ctrl Alt Win AltGr Context [Lock] Ctrl-Alt-Del Local Monitor always on
Windows
Collecting information
Dynamic Update
Preparing installation
Installing Windows
Finalizing installation
Setup will complete in approximately: 39 minutes
The Windows Server 2003 family provides the most productive infrastructure platform for powering networks, applications, and Web services

Bild 197: Überwachung der Windows-Installation im AVR-Fenster

Bei einer Windows-Installation von der Windows Installations-CD/DVD:

Für eine einwandfreie Synchronisation der Mauszeiger müssen Sie auf dem verwalteten Server nach Abschluss der Betriebssystem-Installation folgende Einstellungen anpassen:

- Geschwindigkeit des Mauszeigers
- Hardwarebeschleunigung

Wie Sie dabei im Einzelnen vorgehen, ist beschrieben im Abschnitt „Verwalteter Windows Server: Einstellungen für Mauszeiger-Synchronisation anpassen“ auf Seite 146.

Bei einer Windows-Installation mithilfe des Installation Managers ist die einwandfreie Synchronisation der Mauszeiger automatisch gewährleistet.

11.4.2 Linux nach Konfiguration auf dem verwalteten Server installieren

Die Maus kann während der Linux-Installation verwendet, aber nicht synchronisiert werden.

Bei jedem Wechsel eines Remote Storage-Speichermediums müssen Sie die Remote Storage-Verbindung des aktuell verbundenen Mediums trennen und anschließend das neue Medium als Remote Storage verbinden.

Nach Abschluss der Konfiguration zeigt der Installation Manager folgenden Dialog an:

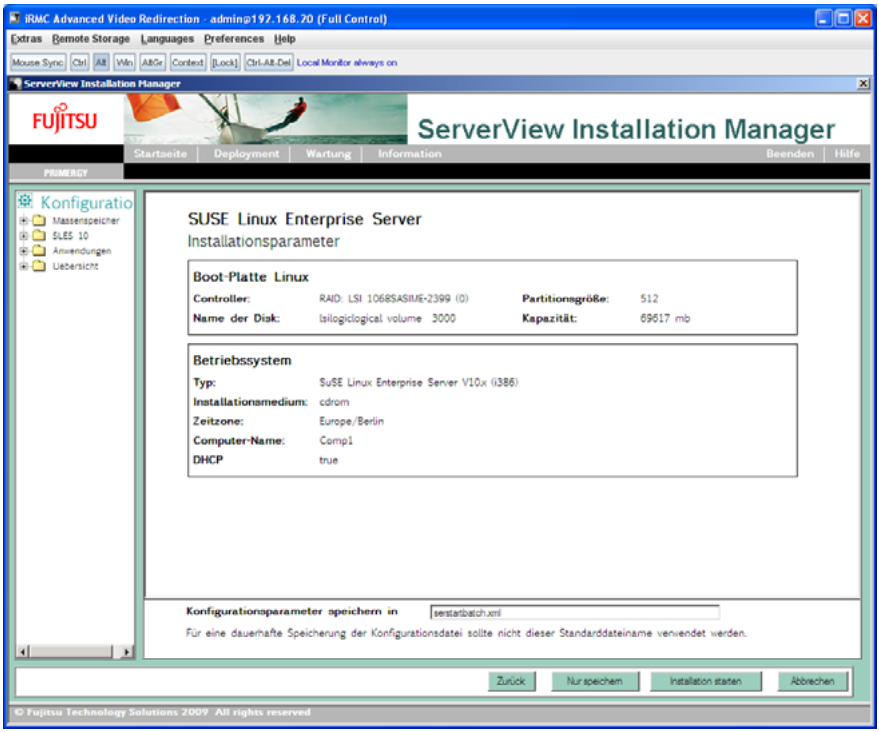


Bild 198: Installation Manager - Installation starten

Wenn Sie als Installationsquelle das lokale CD-ROM/DVD-ROM-Laufwerk des verwalteten Servers konfiguriert haben, gehen Sie am Remote-Arbeitsplatz wie folgt vor:

- Trennen Sie Ihre zurzeit aktiven Remote Storage-Verbindungen. Näheres zum Trennen von Remote Storage-Verbindungen finden Sie auf Seite 167.
- Entfernen Sie die PRIMERGY ServerView Suite DVD 1 aus dem DVD-ROM-Laufwerk am Remote-Arbeitsplatz.
- Legen Sie die Linux Installations-CD/DVD in dieses DVD-ROM-Laufwerk ein.

  Schließen Sie die Anwendung, falls *autostart* aktiviert ist.

- Verbinden Sie das CD-ROM/DVD-ROM-Laufwerk, das die Linux Installations-CD/DVD enthält, als Remote Storage (siehe Seite 165).
- Klicken Sie auf *Installation starten*.

  Alle Installationsdateien werden auf den verwalteten Server kopiert.

  In einem Bestätigungsdialog informiert Sie der Installation Manager über den Abschluss des Kopiervorgangs und fordert Sie auf, vor dem automatischen Neustart des verwalteten Servers alle Speichermedien aus den Wechsellaufwerken zu entfernen.

  Insbesondere müssen Sie vor dem Neustart des Systems auch alle aktiven Remote Storage-Verbindungen trennen.

- Trennen Sie vor dem Neustart des Systems die aktuellen Remote Storage-Verbindungen.

  Verfahren Sie hierfür wie folgt:

  - Starten Sie Remote Storage (siehe Seite 161).

    Es wird die Dialogbox *Storage Devices* mit den aktuell verbundenen Speichermedien und dem Hinweis auf „Safe Remove“ angezeigt (siehe Bild 196 auf Seite 411).

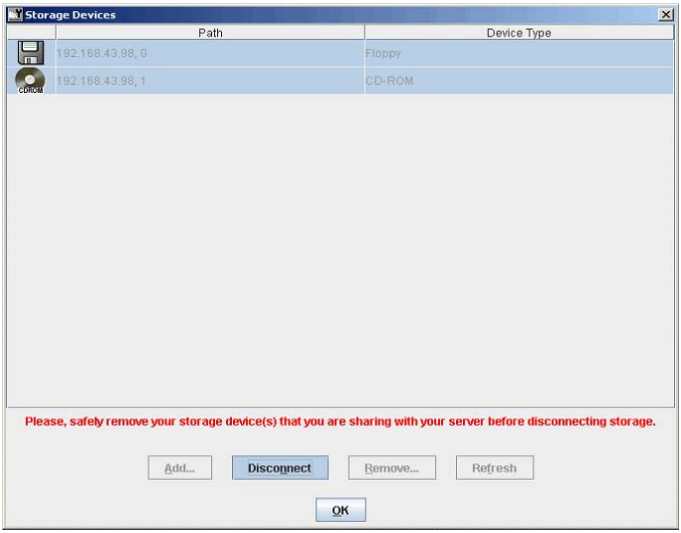


Bild 199: Dialogbox Storage Devices: Remote Storage-Verbindungen trennen

- ► Klicken Sie auf *Disconnect...*, um alle Remote Storage-Verbindungen zu trennen.
- ► Führen Sie einen „Safe Remove“ für die angezeigten Speichermedien durch, d.h. stellen Sie sicher, dass keine Anwendungen/Programme mehr auf die Speichermedien zugreifen.

► Klicken Sie im Bestätigungsdialog auf *Ok*, um den verwalteten Server neu zu starten.

Nach dem Neustart des verwalteten Servers können Sie komplette Installation mithilfe der AVR überwachen (siehe Bild 200 auf Seite 416).

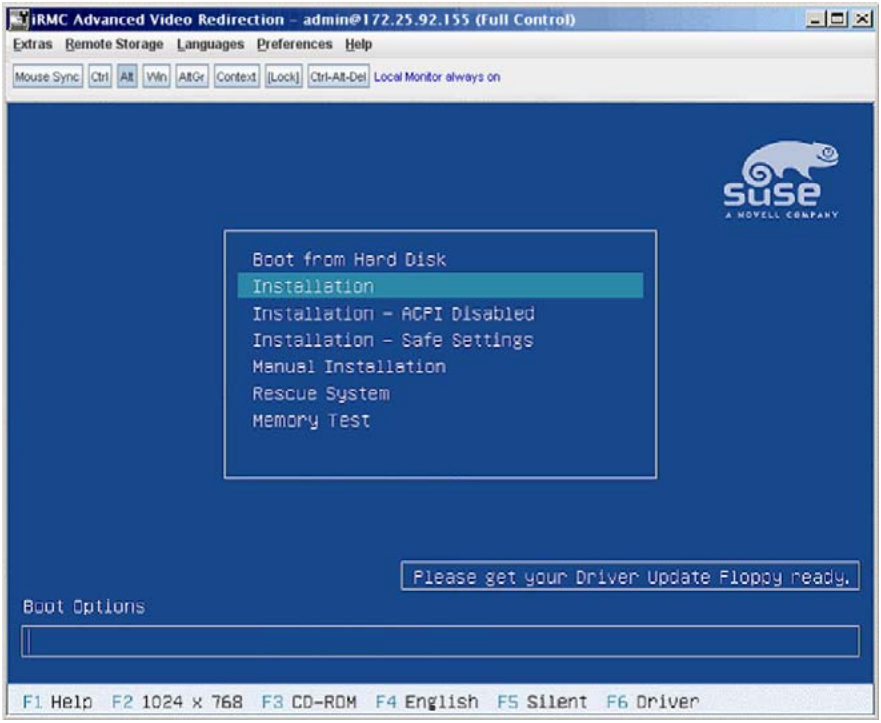

iRMC Advanced Video Redirection - admin@172.25.92.155 (Full Control)
Extras Remote Storage Languages Preferences Help
Mouse Sync Ctrl Alt Win AltGr Context [Lock] Ctrl-Alt-Del Local Monitor always on
Boot from Hard Disk
Installation
Installation - ACPI Disabled
Installation - Safe Settings
Manual Installation
Rescue System
Memory Test
Please get your Driver Update Floppy ready.
Boot Options
F1 Help F2 1024 x 768 F3 CD-ROM F4 English F5 Silent F6 Driver

Bild 200: Verwalteter Server wird von der Linux Installations-CD gebootet.

Nach Abschluss des Bootvorgangs wird der folgende Dialog angezeigt:

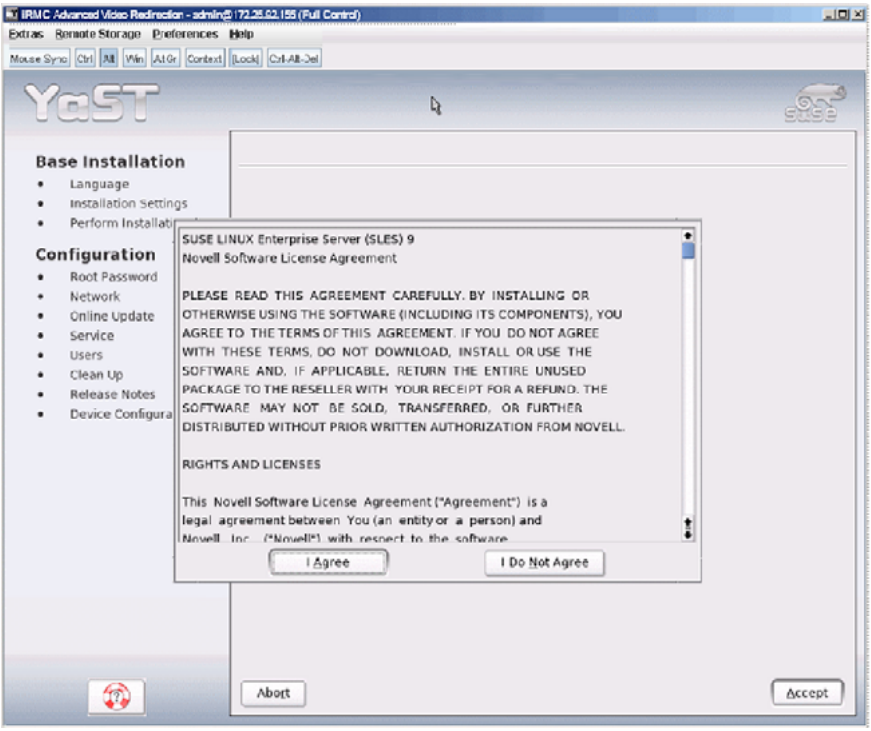

Extras Remote Storage Preferences Help
Mouse Sync Ctrl Alt Win AltGr Context Lock Ctrl-Alt-Del
YaST
Base Installation
Language
Installation Settings
Configuration
Root Password
Network
Online Update
Service
Users
Clean Up
Release Notes
SUSE LINUX Enterprise Server (SLES) 9
Novell Software License Agreement
PLEASE READ THIS AGREEMENT CAREFULLY. BY INSTALLING OR OTHERWISE USING THE SOFTWARE (INCLUDING ITS COMPONENTS), YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE WITH THESE TERMS, DO NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE AND, IF APPLICABLE, RETURN THE ENTIRE UNUSED PACKAGE TO THE RESELLER WITH YOUR RECEIPT FOR A REFUND. THE SOFTWARE MAY NOT BE SOLD, TRANSFERRED, OR FURTHER DISTRIBUTED WITHOUT PRIOR WRITTEN AUTHORIZATION FROM NOVELL.
RIGHTS AND LICENSES
This Novell Software License Agreement ("Agreement") is a legal agreement between You (an entity or a person) and
I Agree
I Do Not Agree
Abort
Accept

Bild 201: Linux Installation - License Agreement

Für eine einwandfreie Synchronisation der Mauszeiger müssen Sie auf dem verwalteten Server nach Abschluss der Betriebssystem-Installation die erforderlichen Einstellungen anpassen. Wie Sie dabei im Einzelnen vorgehen, ist beschrieben im Abschnitt „Verwalteter Linux Server: Einstellungen für Mauszeiger-Synchronisation anpassen“ auf Seite 149.

12 IPMI OEM-Kommandos

In diesem Abschnitt ist eine Auswahl an OEM-spezifischen IPMI-Kommandos beschrieben, die der iRMC unterstützt.

12.1 Überblick

Folgende IPMI OEM-Kommandos werden vom iRMC unterstützt:

- **SCCI-konforme Power ON/OFF-Kommandos**
  (SCCI: **S**erverView **C**ommon **C**ommand **I**nterface)
  - 0115 Get Power On Source
  - 0116 Get Power Off Source
  - 011C Set Power Off Inhibit
  - 011D Get Power Off Inhibit
  - 0120 Set Next Power On Time
- **SCCI-konforme Kommunikationskommandos**
  - 0205 System OS Shutdown Request
  - 0206 System OS Shutdown Request and Reset
  - 0208 Agent Connect Status
  - 0209 Shutdown Request Cancelled
- **SCCI-konformes Signalkommando**
  - 1002 Write to System Display
- **Firmware-spezifische Kommandos**
  - 2004 Set Firmware Selector
  - 2005 Get Firmware Selector
  - C019 Get Remote Storage Connection
  - C01A Set Video Display on/off

- **BIOS-spezifisches Kommando**
  - F109 Get BIOS POST State
  - F115 Get CPU Info
- **iRMC-spezifische Kommandos**
  - F510 Get System Status
  - F512 Get EEPROM Version Info
  - F543 Get SEL entry long text
  - F545 Get SEL entry text
  - F5B0 Set Identify LED
  - F5B1 Get Identify LED
  - F5B3 Get Error LED
  - F5DF Set Nonvolatile Cfg Memory to Default Values
  - F5E0 Set Configuration Space to Default Values
  - F5F8 Delete User ID

12.2 Beschreibung der IPMI OEM-Kommandos

Nachfolgend sind die OEM-spezifischen IPMI-Kommandos im Einzelnen beschrieben.

12.2.1 Beschreibungsformat

Die OEM-spezifischen IPMI-Kommandos dieses Kapitels sind in dem Format beschrieben, das der IPMI-Standard für die Beschreibung der IPMI-Kommandos verwendet.

Der IPMI-Standard beschreibt die IPMI-Kommandos in Form von Kommando-Tabellen, in denen die Eingabe- und Ausgabeparameter des betreffenden Kommandos aufgelistet sind.

Informationen zu den IPMI-Standards finden Sie im Internet:

http://developer.intel.com/design/servers/ipmi/index.htm

12.2.2 SCCI-konforme Power On/Off-Kommandos

01 15 - Get Power On Source

Dieses Kommando informiert über die Ursache des zuletzt durchgeführten „Power On“.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**01** Cmd : Command Group Communication
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**15** Command Specifier
Response Data	-	**BC**
	-	**01**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	3	**01** Länge der Daten
	4	Power on Source: Ursache des letzten Power On

Ursache für Power On	Bedeutung
0x00	Software oder Kommando
0x01	Netzschalter (auf der Frontseite des Servers oder auf der Tastatur)
0x02	Automatischer Restart nach Stromausfall
0x03	Uhr oder Timer (Hardware Real-Time Clock (RTC) oder Software Timer)
0x04	Automatischer Restart nach Shutdown aufgrund eines Lüfterausfalls
0x05	Automatischer Restart nach Shutdown aufgrund kritischer Temperatur
0x08	Reboot nach Watchdog Timeout
0x09	Einschalten vom Remote-Arbeitsplatz aus (Modem RI Line, SCSI Termination Power, LAN Chip-Kartenleser etc.)
0x0C	Reboot nach CPU-Fehler
0x15	Reboot durch Hardware-Reset
0x16	Reboot nach Warmstart
0x1A	Eingeschaltet durch ein Ereignis (Event) des PCI BUS Power Management
0x1D	Eingeschaltet via Remote Manager vom Remote-Arbeitsplatz aus
0x1E	Reboot/Reset via Remote Manager vom Remote-Arbeitsplatz aus

01 16 - Get Power Off Source

Dieses Kommando informiert über die Ursache des zuletzt durchgeführten „Power Off“.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**01** Cmd : Command Group Communication
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**16** Command Specifier
Response Data	-	**BC**
	-	**01**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS LS Byte first
	3	**01** Länge der Daten
	4	Power off Source: Ursache des letzten Power Off

Ursache für Power Off	Bedeutung
0x00	Software (SWOFF, SE: Power OFF per Kommando)
0x01	Netzschalter (auf der Frontseite des Servers oder auf der Tastatur)
0x02	Stromausfall
0x03	Uhr oder Timer (Hardware Real-Time Clock (RTC) oder Software Timer)
0x04	Lüfterausfall
0x05	Kritische Temperatur
0x08	Finales Ausschalten nach wiederholtem Watchdog Timeout
0x0C	Finales Ausschalten nach wiederholtem CPU-Fehler
0x1D	Ausgeschaltet via Remote Manager vom Remote-Arbeitsplatz aus

01 1C - Set Power Off Inhibit

Dieses Kommando setzt das *Power Off Inhibit*-Flag, mit dem ein willkürliches Ausschalten des Servers temporär verhindert werden kann.

Bei gesetztem *Power Off Inhibit*-Flag speichert die Firmware die Ursache für einen willkürlich versuchten „Power Off“, „Power Cycle“ oder Server-Neustart, führt die entsprechende Aktion jedoch nicht aus. Aktuell gespeichert ist dabei immer die Ursache für den zuletzt initiierten „Power Off“-, „Power Cycle“- oder Neustart-Versuchs. Die gespeicherte Aktion wird erst nach dem Rücksetzen des *Power Off Inhibit*-Flags ausgeführt.

Das *Power Off Inhibit*-Flag wird nach einem Stromausfall oder bei Betätigung der Reset-Taste automatisch zurückgesetzt.

In seiner Wirkung entspricht *Power Off Inhibit*-Flag dem Dump-Flag, das bei Erstellen eines Hauptspeicher-Dumps benutzt wird. Hier muss der Initiator vor dem Ziehen des Dumps das Flag setzen und nach Dump-Erstellung wieder zurücksetzen.

Request Data	-	**B8** NetFn|LUN: OEM/Group
	-	**01** Cmd : Command Group Communication
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**1C** Command Specifier
	5	**00** Object ID
	6:7	**00 00** Value ID
	8	**01** Länge der Daten
	9	Power Off Inhibit Flag: 0 no Inhibit, 1 Inhibit
Response Data	-	**BC**
	-	**01**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first

01 1D - Get Power Off Inhibit

Dieses Kommando ermittelt den Wert des *Power Off Inhibit*-Flags.

Näheres zum *Power Off Inhibit*-Flag siehe Beschreibung zu
„01 1C - Set Power Off Inhibit“ auf Seite 424.

Request Data	-	**B8** NetFn|LUN: OEM/Group
	-	**01** Cmd : Command Group Communication
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**1D** Command Specifier
Response Data	-	**BC**
	-	**01**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	5	**01** Länge der Antwort-Daten
	6	Power Off Inhibit Flag: 0 no Inhibit, 1 Inhibit

01 20 - Set Next Power On Time

Dieses Kommando veranlasst das Einschalten des Servers zum spezifizierten Zeitpunkt, unabhängig von den im Configuration Space konfigurierten Ein-/Ausschalt-Zeiten.

Das Kommando bewirkt nur ein einmaliges Ausschalten

Einen zuvor per 01 20-Kommando Time festgelegten „Power On“-Zeitpunkt annulieren Sie, indem Sie mit einem nachfolgenden 01 20-Kommando den Power On-Zeitpunkt „0“ spezifizieren.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**01** Cmd : Command Group Communication
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**20** Command Specifier
	5	**00** Object ID
	6:7	**00 00** Value ID
	8	**04** Länge der Daten
	9:12	Time (LSB first) (siehe unten)
Response Data	-	**BC**
	-	**01**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first

Time (LSB first)

Zeitpunkt, dargestellt im UNIX-spezifischen Format, zu dem der Server sich wieder einschalten soll. Das Granulat für die Zeitangabe ist eine Minute. Die Zeitangabe wird **nicht** nicht-flüchtig gespeichert. Nach Einschalten des Servers zum spezifizierten Zeitpunkt wird die Zeitangabe intern auf 0 gesetzt.
Bei Angabe Time == 0 wird der Server nicht eingeschaltet.

12.2.3 SCCI-konforme Kommunikationskommandos

Die SCCI-konformen Kommunikationskommandos setzen voraus, dass der Agent-Service unter dem Server-Betriebssystem läuft. Für die Ausführung der Kommandos kommuniziert der iRMC mit dem SCCI-Agenten, der die Aktion dann ausführt.

02 05 - System OS Shutdown Request

Dieses Kommando initiiert den Shutdown des Server-Betriebssystems.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**02** Cmd : Command Group Communication
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**05** Command Specifier
Response Data	-	**BC**
	-	**02**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first

02 06 - System OS Shutdown Request and Reset

Dieses Kommando initiiert den Shutdown und anschließenden Reset des Server-Betriebssystems.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**02** Cmd : Command Group Communication
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**06** Command Specifier
Response Data	-	**BC**
	-	**02**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first

02 08 - Agent Connect Status

Dieses Kommando prüft, ob der SCCI-Agent aktiv ist.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**02** Cmd : Command Group Communication
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**08** Command Specifier
Response Data	-	**BC**
	-	**02**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	5	**01** Data Length
	6	Connect status Status der Verbindung: 00: Verbindung verloren, keine Verbindung zum Agenten. 01: Verbindung wiederhergestellt, Verbindung zum Agenten exisitiert.

02 09 - Shutdown Request Cancelled

Dieses Kommando annulliert einen aktuellen Shutdown-Request.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**02** Cmd : Command Group Communication
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**09** Command Specifier
Response Data	-	**BC**
	-	**02**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first

12.2.4 SCCI-konformes Signalkommando

10 02 - Write to System Display

Dieses Kommando gibt Text auf ein angeschlossenes LocalView Display aus.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**10** Cmd : Command Group Fan Test
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**02** Command Specifier
	5	**Object Index**: Zeile auf dem Display, in die geschrieben werden soll.
	6:7	**Value ID** (nicht verwendet)
	8	**Length** Anzahl der zu schreibenden Zeichen + 1. (Der String braucht nicht durch das NULL-Byte terminiert zu sein. Falls die die Länge des Displays für die Darstellung des Strings nicht ausreicht, werden überzählige Zeichen abgeschnitten.)
	9	Attribut: 0 = String linksbündig schreiben 1 = String zentriert schreiben
	10:10+n	**Zeichen**, die auf das Display geschrieben werden sollen. Der String braucht nicht durch das NULL-Byte terminiert zu sein.
Response Data	-	**BC**
	-	**10**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first

12.2.5 Firmware-spezifische Kommandos

20 04 - Set Firmware Selector

Dieses Kommando konfiguriert, welches Firmware Image des iRMC nach einem Firmware-Reset aktiv ist.

Request Data	-	**20** NetFnlLUN: Firmware
	-	**04** CMD : Command Group Firmware
	1	Selector: 0 = Auto (Firmware Image mit der neuesten Firmware-Version) 1 = low Firmware Image 2 = high Firmware Image 3 = Auto oldest version (Firmware Image mit der ältesten Firmware-Version) 4 = MRP (Firmware Image mit der zuletzt aktualisierten Firmware) 5 = LRP (Firmware Image mit der am längsten nicht mehr aktualisierten Firmware)
Response Data	-	**24**
	-	**04**
	1	Completion Code

20 05 - Get Firmware Selector

Dieses Kommando liefert die Einstellungen des aktuellen Firmware Selectors .

Request Data	-	**20** NetFnlLUN: Firmware
	-	**05** CMD : Command Group Firmware
Response Data	-	**24**
	-	**05**
	1	Completion Code
	2	Next Boot Selector: 0 = Auto (EEPROM mit der neuesten Firmware-Version) 1 = low EEPROM 2 = high EEPROM 3 = Auto oldest version (EEPROM mit der ältesten Firmware-Version) 4 = MRP (EEPROM mit der zuletzt aktualisierten Firmware) 5 = LRP(EEPROM mit der am längsten nicht mehr aktualiserten Firmware)
	3	Running Selector; zeigt an, welcher EEPROM aktiv ist: 1 = low EEPROM 2 = high EEPROM

C0 19 - Get Remote Storage Connection or Status

Dieses Kommando informiert je nach Parametrisierung,

– ob Remote Storage-Verbindungen bestehen,
– über Status und Typ der Remote Storage-Verbindung(en).

Wenn *Request Data 1* auf 1 gesetzt ist, informiert das Kommando, ob Speichermedien als Remote Storage verbunden sind.

Request Data	-	**C0** NetFnlLUN: OEM
	-	**19** CMD : Command Group Firmware
	1	01
	2	00
	3	00
Response Data	-	**C4**
	-	**19**
	1	Completion Code
	2	**01**
	3	**00: No** **01: Yes, connected**
	4	**00**
	5	**00**

Wenn *Request Data 1* auf 2 gesetzt ist, informiert das Kommando über Status und Typ der Remote Storage-Verbindung(en).

Request Data	-	**C0** NetFnlLUN: OEM
	-	**19** CMD : Command Group Firmware
	1	02
	2	00
	3	00 = Connection 0 01 = Connection 2
Response Data	-	**C4**
	-	**19**
	1	Completion Code
	2	**02**
	3	**00**
	4	**00**
	5	00 **= Invalid / unknown** **01 = Idle** **02 = Connection Attempt pending** **03 = Connected** **04 = Connection Attempts retries exhausted / failed** **05** = **Connection lost** **06** = **Disconnect pending**
	6	00 **= Invalid / unknown** **01 = Storage Server / IPMI** **02 = Applet** **03 = None / Not connected**

C0 1A - Set Video Display On/Off

Dieses Kommando ermöglicht das Ein- und Ausschalten der lokalen Konsole.

Request Data	-	**C0** NetFnlLUN: OEM
	-	**1A** Cmd : Command Group Firmware
	1	00 = Set Video Display On 01 = Set Video display Off
Response Data	-	**C4**
	-	**1A**
	1	Completion Code

12.2.6 BIOS-spezifische Kommandos

F1 09 - Get BIOS POST State

Dieses Kommando informiert, ob sich das BIOS in der POST-Phase befindet.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F1** Cmd : Command Group BIOS
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**09** Command Specifier
Response Data	-	**BC**
	-	**F1**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	5	[7:1] - reserved [0] - BIOS POST State : 0 = BIOS is not in POST 1 = BIOS is in POST

F1 15 - Get CPU Info

Dieses Kommando liefert CPU-interne Informationen. Der iRMC empfängt diese Information während der POST-Phase das BIOS.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F1** Cmd : Command Group BIOS
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**15** Command Specifier
	5	Socket Number (0-based) of the CPU
Response Data	-	**BC**
	-	**F1**
	1	Completion Code: 01 = Unpopulated CPU Socket
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	5:6	CPU ID, LS Byte first
	7	Platform ID
	8	Brand ID
	9:10	Maximal Core Speed of the CPU [MHz], LS Byte first
	11:12	Intel Qickpath Interconnect in Mega Transactions per second, LS Byte first
	13	T-Control Offset
	14	T-Diode Offset
	15	CPU data Spare
	16:17	Record ID CPU Info SDR, LS Byte first
	18:19	Record ID Fan Control SDR, LS Byte first
	20:21	CPU ID High Word, LS Byte first (0 if none)

12.2.7 iRMC-spezifische Kommandos

F5 10 - Get System Status

Dieses Kommando liefert eine Vielzahl interner Informationen über den Server, wie z.B Power- oder Fehlerstatus.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd: Command Group Memory
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	10 Command Specifier
	5:8	**Timestamp**
Response Data	-	**BC**
	-	**F5**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	5	**System Status** (Details siehe unten.)
	6	**Signaling** (Details siehe unten.)
	7	**Notifications** (Details siehe unten.)
	8	**POST Code**

Der Zeitstempel (*Timestamp*) wird nur für die Auswertung des *Notifications*-Byte benötigt.

System Status

Bit 7 - System ON

Bit 6 -

Bit 5 -

Bit 4 - SEL entries available

Bit 3 -

Bit 2 - Watchdog active

Bit 1 - Agent connected

Bit 0 - Post State

Signaling

Bit 7 - Localize LED

Bit 6 -

Bit 5 -

Bit 4 -

Bit 3 -

Bit 2 -

Bit 1 - Global Error LED

Bit 0 - Global Error LED

Notifications

Bit 7 - SEL Modified (New SEL Entry)

Bit 6 - SEL Modified (SEL Cleared)

Bit 5 - SDR Modified

Bit 4 - Nonvolatile IPMI Variable modified

Bit 3 - ConfigSpace Modified

Bit 2 -

Bit 1 -

Bit 0 - New Output on LocalView panel

F5 12 - Get EEPROM Version Info

Dieses Kommando informiert über die aktuellen Versionen von Bootloader, Firmware und SDR in den EEPROMs.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : Command Group Memory
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	12 Command Specifier
	5	EEPROM# 00=EEPROM 1; 01=EEPROM 2
Response Data	-	**BC**
	-	**F5**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	5	**Status** 00=Checksum Error Runtime FW, 01=OK
	6	**Major FW Revision** Binary coded
	7	**Minor FW Revision** BCD coded
	8:10	**Aux. FW Revision** Binary coded (major/minor/res.)
	11	**Major FW Revision** ASCII coded letter
	12	**Major SDRR Revision** BCD coded
	13	**Minor SDRR Revision** BCD coded
	14	**SDRR Revision Char.** ASCII coded letter
	15	**SDRR-ID** LSB binary coded
	16	**SDRR-ID** MSB binary coded
	17	**Major Booter Revision** Binary coded
	18	**Major Booter Revision** BCD coded
	19:20	**Aux. Booter Revision** Binary coded (major/minor)

F5 43 - Get SEL entry long text

Dieses Kommando übersetzt einen vorliegenden System Event Log (SEL) in Klartext.

Request Data	-	**B8** NetFn|LUN: OEM/Group
	-	**F5** Cmd : Command Group iRMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**43** Command Specifier
	5:6	**Record ID** of SEL record, LS Byte first 0x0000: get first record 0xFFFF: get last record
	7	**Offset** in response SEL text
	8	**MaxResponseDataSize** size of **Converted SEL data** (16:n) in response
Response Data	-	**BC**
	-	**F5**
	1	Completion Code:
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	5:6	**Next Record ID**
	7:8	**Actual Record ID**
	9	**Record type**
	10:13	**Timestamp**
	14	**Severity:** Bit 7: 0 = No CSS component 1 = CSS component Bit 6-4: 000 = INFORMATIONAL 001 = MINOR 010 = MAJOR 011 = CRITICAL 1xx = Unknown' Bit 3-0: reserved, read as 0000
	15	**Data length** of the whole text
	16:n	**Converted SEL data** requested part (n = 16 + MaxResponseDataSize - 1)
	n + 1	**String Terminator** trailing '\0' character

F5 45 - Get SEL entry text

Dieses Kommando übersetzt einen vorliegenden System Event Log (SEL) in ASCII-Text.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : Command Group iRMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**45** Command Specifier
	5:6	**Record ID** of SDR, LS Byte first
Response Data	-	**BC**
	-	**F5**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	5:6	**Next Record ID**
	7:8	**Actual Record ID**
	9	**Record type**
	10:13	**Timestamp**
	14	**Severity:** Bit 7: 0 = No CSS component 1 = CSS component Bit 6-4: 000 = INFORMATIONAL 001 = MINOR 010 = MAJOR 011 = CRITICAL 1xx = Unknown' Bit 3-0: reserved, read as 0000
	15	**Data length**
	16:35	**Converted SEL data**

F5 B0 - Set Identify LED

Mithilfe dieses Kommandos können Sie die Identifizierungs-LED (blau) des Servers ein- und ausschalten.

Die Identify LED können Sie außerdem über den Identify Button am Servers ein- und ausschalten.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : Command Group BIOS
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	B0 Command Specifier
	5	Identify LED: 0: Identify LED aus 1: Identify LED an
Response Data	-	**BC**
	-	**F5**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first

F5 B1 - Get Identify LED

Dieses Kommando informiert über den Status der Identifizierungs-LED (blau) des Servers, unabhängig davon, ob die Identify LED per F5 B0-Kommando oder mithilfe des Identify Button gesetzt wurde.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : Command Group BIOS
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	B1 Command Specifier
Response Data	-	**BC**
	-	**F5**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	5	Status der Identify LED (nur Bit 0 ist relevant)

F5 B3 - Get Error LED

Dieses Kommando informiert über den Status der Global Error LED (rot) des Servers. Die Global Error LED zeigt die schwerwiegendsten Fehler-Status der Komponenten an.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : Command Group BIOS
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	B3 Command Specifier
Response Data	-	**BC**
	-	**F5**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	5	Status der Error LED: 0: Error LED ausgeschaltet. 1: Error LED eingeschaltet. 2: Error LED blinkt.

F5 DF - Reset Nonvolatile Cfg Variables to Default

Dieses Kommando setzt alle nicht-flüchtigen IPMI Settings auf Default-Werte.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : Command Group Configuration
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	DF Command Specifier
	5:8	43 4C 52 AA = 'CLR'0xaa : Security Code
Response Data	-	**BC**
	-	**F5**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first

F5 E0 - Reset ConfigSpace Variables to Default

Dieses Kommando setzt alle Variablen des Configuration Space auf Default-Werte.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : Command Group Configuration
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	E0 Command Specifier
	5:8	43 4C 52 AA = 'CLR'0xaa : Security Code
Response Data	-	**BC**
	-	**F5**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first

F5 F8 - Delete User ID

Mit diesem Kommando können Sie iRMC-Benutzerkennungen löschen.

ACHTUNG!

Wenn Sie alle Benutzerkennungen löschen, kann der iRMC nicht mehr bedient werden.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : Command Group iRMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	F8 Command Specifier
	5:8	User ID (1-16)
Response Data	-	**BC**
	-	**F5**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first

Literatur

Die Dokumentationen der PRIMERGY-Handbücher finden Sie auf der PRIMERGY ServerView Suite DVD 2, die mit jedem Serversystem ausgeliefert wird.

Die Dokumentationen sind auch über das Internet als Download kostenlos erhältlich. Die Online-Dokumentation zur PRIMERGY ServerView Suite finden Sie unter *http://manuals.ts.fujitsu.com* und dem Link *Industry standard servers*.

[1] **ServerView Suite**
Grundlegende Konzepte

[2] **PRIMERGY Glossar**

[3] **PRIMERGY Abkürzungen**

[4] **Sicheres PRIMERGY Server Management**
Enterprise Security
PRIMERGY Server Management
Sicherheit für hochverfügbare Plattformen
White Paper

[5] **PRIMERGY ServerView Suite**
Installation Manager
Benutzerhandbuch

[6] **PRIMERGY ServerView Suite**
Deployment Manager
Benutzerhandbuch

[7] **PRIMERGY ServerView Suite**
ServerView Operations Manager
Installation unter Windows
Installationshandbuch

[8] **PRIMERGY ServerView Suite**
ServerView Operations Manager
Installation unter Windows
Installationskurzanleitung

[9] **PRIMERGY ServerView Suite**
ServerView Operations Manager
Installation unter Linux
Installationshandbuch

[10] **PRIMERGY ServerView Suite**
ServerView Operations Manager
Installlation unter Linux
Installationskurzanleitung

[11] **PRIMERGY ServerView Suite**
ServerView S2
ServerView-Agenten (Linux und VMware)
Installationskurzanleitung

[12] **PRIMERGY ServerView Suite**
ServerView Operations Manager
Server Management
Benutzerhandbuch

[13] **PRIMERGY ServerView Suite**
ServerView Inventory Manager
Benutzerhandbuch

[14] **PRIMERGY ServerView Suite**
ServerView Archive Manager
Benutzerhandbuch

[15] **PRIMERGY ServerView Suite**
Asset Management
Kommandoschnittstelle
Benutzerhandbuch

[16] **PRIMERGY ServerView Suite**
ServerView RAID Manager
Benutzerhandbuch

[17] **PRIMERGY ServerView Suite**
ServerView Event Manager
Benutzerhandbuch

[18] **PRIMERGY ServerView Suite**
ServerView Threshold Manager
Benutzerhandbuch

[19] **PRIMERGY ServerView Suite**
ServerView Performance Manager
Benutzerhandbuch

[20] **PRIMERGY ServerView Suite**
ServerView Download Manager
ServerView
Benutzerhandbuch

[21] **PRIMERGY ServerView Suite**
ServerView Update Manager
Benutzerhandbuch

[22] **PRIMERGY ServerView Suite**
ServerView Update Manager Express
Benutzerhandbuch

[23] **PRIMERGY ServerView Suite**
PrimeUp
Benutzerhandbuch

[24] **PRIMERGY ServerView Suite**
Bootable Update CD
Benutzerhandbuch

[25] **PRIMERGY ServerView Suite**
ServerView Online Diagnostics
Benutzerhandbuch

[26] **PRIMERGY ServerView Suite**
Local Service Concept (LSC)
Benutzerhandbuch

[27] **PRIMERGY ServerView Suite**
PrimeCollect
Benutzerhandbuch

[28] **PRIMERGY ServerView Suite**
ServerView Virtual-IO Manager
Benutzerhandbuch

[29] **PRIMERGY ServerView Suite**
ServerView Virtual-IO Manager CLI
Command Line Interface

[30] **PRIMERGY ServerView Suite**
ServerView Integration
Überblick

[31] **PRIMERGY ServerView Suite**
ServerView Integration in MOM
Benutzerhandbuch

[32] **PRIMERGY ServerView Suite**
ServerView Integration Pack für MS SCOM
Benutzerhandbuch

[33] **PRIMERGY ServerView Suite**
ServerView Integration Pack for MS SMS
Benutzerhandbuch

[34] **PRIMERGY ServerView Suite**
DeskView und ServerView Integration Pack für Microsoft SCCM
Benutzerhandbuch

[35] **PRIMERGY ServerView Suite**
ServerView Integration in HP OpenView NNM
Benutzerhandbuch

[36] **PRIMERGY ServerView Suite**
ServerView Integration in HP Operations Manager
Benutzerhandbuch

[37] **PRIMERGY ServerView Suite**
ServerView Integration Pack in Tivoli NetView
Benutzerhandbuch

[38] **PRIMERGY ServerView Suite**
ServerView Integration Pack in Tivoli TEC
Benutzerhandbuch

[39] **PRIMERGY ServerView Suite**
ServerView Integration in DeskView
Benutzerhandbuch

[40] **PRIMERGY ServerView Suite**
ServerView Remote Management Frontend
Benutzerhandbuch

[41] **PRIMERGY ServerView Suite**
iRMC - integrated Remote Management Controller
Benutzerhandbuch

[42] **PRIMERGY ServerView Suite**
iRMC S2 - integrated Remote Management Controller
Benutzerhandbuch

[43] **PRIMERGY BX300 Blade Server Systems**
Operating Manual

[44] **PRIMERGY BX600 Blade Server Systems**
Operating Manual

[45] **PRIMERGY BX600 Blade Server Systems**
ServerView Management Blade S3
User Interface Description
User Guide

[46] **PRIMERGY BX900 Blade Server Systems**
Operating Manual

[47] **PRIMERGY BX900 Blade Server Systems**
ServerView Management Blade S1
User Interface Description
User Guide

[48] **PRIMERGY Blade Server Systems**
LAN Switch Blade
User Interface Description
User Guide

[49] **BIOS-Setup**
Beschreibung

[50] **PRIMEPOWER ServerView Suite**
Rechnerverwaltung in einer Domäne
Benutzerhandbuch

[51] **FibreCAT CX**
FibreCAT CX-Systeme mit ServerView Operations Manager überwachen
Kurzanleitung

[52] **FibreCAT SX**
FibreCAT SX-Systeme mit ServerView Operations Manager überwachen
Kurzanleitung

[53] **StorMan**
Provisioning and managing virtualized storage resources
Administrator and User Guide

[54] **APC network management card**
User's Guide

[55] **VMware**
VMware ESX Server
Installation Guide

[56] **VMware**
VMware ESX Server
Administration Guide

Stichwörter

A

abfragen
- Infos zu Server-Komponenten 194
- Infos zum Server 191
- iRMC-Informationen 196
- Server Management Informationen 233
- Systeminformationen 190

Active Directory 18, 59, 68, 369
- iRMC-Gruppen und Benutzerrechte 91
- Konfiguration über iRMC-Web-Oberfläche 276
- Konfiguration über Server Configuration Manager 369

Advanced Features 374
Advanced Video Redirection
- siehe auch AVR

Advanced Video Redirection (AVR) 292
Alarm siehe auch Alerting 355
Alarmbenachrichtigung siehe Alerting
Alerting
- konfigurieren 55, 57, 251, 360

anmelden
- am iRMC (Voraussetzungen) 33
- am Remote Manager 312
- an der iRMC-Web-Oberfläche 35, 182

anzeigen
- aktuelles DSA-Zertifikat 204
- DSA/RSA-Zertifikat 204

ASP 385
ASR&R Fan Settings 342
ASR&R Options konfigurieren 235
ASR&R Temperature Settings 344
aufrufen, Remote Storage Server GUI 176
Ausführungsmodus, Remote Storage Server 175
ausschalten, Server 214
Autonomous Support Package
- siehe ASP

AVR 137
- besondere Tastenkombinationen 142
- integrierte Sondertasten 142
- Local Monitor Off 141
- Menüs 151
- parallele Sitzungen 140
- Secure Keyboard 143
- starten 292
- Umleitung der Maus 144
- Umleitung der Tastatur 140
- verwenden 139
- virtuelle Tastatur 143, 152
- Voraussetzungen prüfen 138

AVR-Fenster
- Menü Extras 151, 152
- Menü Languages 155
- Menü Preferences 156
- Menü Remote Storage 155

B

bedienen
- iRMC über Telnet/SSH 302, 307, 309
- Remote Manager 309

Bedienoberfläche (iRMC) 187
beenden, Remote Storage Server 180
Benutzer
- konfigurieren 263, 265, 361
- konfigurieren (Details) 266
- konfigurieren (neu) 265, 362
- konfigurieren, lokal 263, 361

Benutzerberechtigung 62
- global 70, 72
- in Active Directory 91
- in eDirectory 116
- in OpenLDAP 129

Server-übergreifend 72
Benutzerkennung 30, 59
vorkonfiguriert 63
Benutzerverwaltung (iRMC) 59
Benutzer zu Gruppe zuordnen 91, 120
Benutzerkennung 59
bevorzugte Shell 75
Domain Controller-Zertifikat erzeugen 88
Domain Controller-Zertifikat installieren 90
Enterprise CA installieren 86
global 68
globale Benutzerberechtigung 70, 72
in eDirectory integrieren 112
iRMCgroups im LDAP Directory Service generieren 76
Konzept 60
LDAP-Zugriff konfigurieren 86
lokal 64
lokal über iRMC-Web-Oberfläche 64, 263
lokal über Server Configuration Manager 66, 361
via Active Directory 68, 70
via Directory Service 70
Berechtigung
für spezielle iRMC-Funktionen 63
iRMC-Web-Oberfläche 184
Remote Manager 316
Berechtigung siehe auch Benutzerberechtigung, Privilegien
Berechtigungsgruppe 73
kanal-spezifisch 62
besondere Tastenkombinationen (AVR) 142
Betriebssystem, Remote-Installation 395
siehe auch Remote-Installation des Betriebssystems
BIOS Text Console 281
BIOS Text-Konsolumleitung konfigurieren 44, 45, 281
Boot Options konfigurieren 213
Boot Watchdog 237
booten, iRMC 197

C

CA (Certification Authority) 86
CD-ROM 163
Certification Authority (CA) 86
CLP 328
Benutzerdaten 330
Syntax 328
CLP siehe auch SMASH CLP
Command Line Protocol (CLP) 328
Command Line Shell (Remote Manager) 327
Component Status 226
ConsoleOne
installieren 104
starten 105
Copyright (SSL) 134

D

Darstellungsmittel 32
DHCP Configuration 247
Directory Service 68, 273, 367
Directory Service siehe auch Active Directory, eDirectory, OpenLDAP
DNS Configuration 249
DNS für iRMC konfigurieren 249, 353
DNS Registration 351
DNS Server 353
Dokumentation 15
Domain Controller-Zertifikat 88, 90
DSA-Schlüssel (privat)
auf den iRMC laden 202
direkt eingeben 207
in Datei bereitstellen 206
DSA-Zertifikat
aktuelles anzeigen 204
Default-Zertifikat 202

Default-Zertifikat wiedereinsetzen 205
direkt eingeben 207
DSA/RSA- Schlüssel
Eingabeformat 202
DSA/RSA-Schlüssel
direkt eingeben 207
DSA/RSA-Zertifikat
anzeigen 204
auf den iRMC laden 202
direkt eingeben 207
Eingabeformat 202
DVD-ROM 163

E

E-Mail-Weiterleitung siehe auch Email Alerting
eDirectory 18, 59, 68, 371
für LDAP konfigurieren 107
installieren 99
iRMC-Benutzer der OU iRMC-groups zuordnen 120
iRMC-Gruppen und Benutzerrechte 116
konfigurieren 106
Konfigurieren über Server Configuration Manager 371
LDAP-Authentifizierungsprozess 112
LDIF-Datei importieren 114
Principal User für iRMC erzeugen 116
Software-Komponenten und Systemanforderungen 98
Tipps zur Administration 124
Zugriff via LDAP Browser testen 111
eDirectory Server
installieren 100
EEPROM, iRMC 378
eingeben
DSA-Zertifikat 207
DSA/RSA-Schlüssel 207
einschalten, Server 214
einsehen, System Event Log (Server) 230
EMail Alerting 355
Email Alerting konfigurieren 256, 355
Email Configuration 270
Emergency Mode 390
Enclosure Information (Remote Manager) 321
Enterprise CA 86
erzeugen
selbstsigniertes Zertifikat 208
Ethernet 240
Ethernet-Einstellungen (iRMC) konfigurieren 240, 346

F

Fan siehe auch Lüfter
Fan Test 220
Fan testen 220
Fans 220
Farbcode (Sensor) 219
Fehler-Icon 227
Firmware Selector, iRMC 379
Firmware, iRMC 378
Firmware-Update 377
Offline-Update 387
Online-Update 384
Operanden 391
Flash siehe auch Firmware-Update
Flash-Tool
Offline-Update (Firmware) 389
Online-Update (Firmware) 385
Flash-Tools
flbmc 389
RedhatFLBMC 385
SuseFLBMC 385
Syntax und Operanden 391
WinFLBMC 385
FlashDisk-Menü
Offline-Update (Firmware) 388
flbmc
Offline-Update (Firmware) 389

Floppy-Disk 163
Funktionen, iRMC 16

G
Gerätetyp (Remote Storage) 163
Global Email Paging
  Configuration 258
Global Error LED 192
globale Benutzerkennung 59
globale iRMC-
  Benutzerverwaltung 68
  via Active Directory 80
  via eDirectory 98
  via OpenLDAP 127

H
Hauptmenü (Remote Manager) 314
Host-Name (iRMC) 351
  konfigurieren 247, 351
  siehe auch iRMC-Name
HP SIM-Integration
  konfigurieren 238, 375

I
ICMB 24
Identifizierungs-LED 192, 325
Image-File (ISO Image) 163, 169
iManager
  einloggen 103
  installieren 102
Informationen abfragen
  Infos zum RMC 196
  Infos zum Server 191
  iRMC-Firmware 197
  Server-Komponenten 194
  Spannungssensoren 224
  Stromversorgung 225
  System Event Log 231
installieren
  Betriebssystem 395
  ConsoleOne 104
  eDirectory 99
  eDirectory Administrations-Utilities 100
  eDirectory Server 100
  iManager 102
  Linux 413
  OpenLDAP 127
  Remote Storage Server 170
  siehe auch Remote-Installation des Betriebssystems
  Windows 409
integrierte Sondertasten (AVR) 142
Intelligent Platform Management Interface, siehe IPMI
IPMB 24
IPMI
  Benutzerkennungen 30
  Definition 22
  Hintergrund 22
  Implementierung 24
  IPMI-over-LAN-Schnittstelle 27
  Kanal-Konzept 29
  Referenzen 30
  Serial Over LAN (SOL) 28
  Standards 24
IPMI OEM-Kommandos 419
  0115 - Get Power On Source 422
  0116 - Get Power Off Source 423
  011C - Set Power Off Inhibit 424
  011D - Get Power Off Inhibit 425
  0120 - Set Next Power On Time 426
  0205 - System OS Shutdown Request 427
  0206 - System OS Shutdown Request and Reset 427
  0208 - Agent Connect Status 428
  0209 - Shutdown Request Cancelled 428
  1002 - Write to System Display 429
  2004 - Set Firmware Selector 430
  2005 - Get Firmware Selector 431
  Beschreibungsformat 421

C019 - Get Remote Storage Connection or Status 432
C01A - Set Video Display On/Off 433
F109 - Get BIOS POST State 434
F115 - Get CPU Info 435
F510 - Get System Status 436
F512 - Get EEPROM Version Info 438
F543 - Get SEL entry long text 439
F545 - Get SEL entry text 440
F5B0 - Set Identify LED 441
F5B1 - Get Identify LED 441
F5B3 - Get Error LED 442
F5DF - Reset Nonvolatile Cfg Variables to Default 443
F5E0 - Reset ConfigSpace Variables to Default 443
F5F8 - Delete User ID 444
Überblick 419
iRMC 21
Advanced Video Redirection (AVR) 292
an der Web-Oberfläche anmelden 35, 182
anmelden (Voraussetzungen) 33
AVR 137
Bedienoberfläche 187
Benutzerberechtigungen 62
Benutzerverwaltung 59
Berechtigung 63
EEPROM 378
Firmware 378
Firmware-Einstellungen 200
Firmware-Selector 379
Firmware-Update 377
Funktionen 16
Kommunikationsschnittstellen 21
konfigurieren 37
LAN-Schnittstelle konfigurieren 38, 41, 54, 56, 239
LAN-Schnittstelle testen 43
License Key 137, 159
Local Monitor Off 141, 293
neu starten 197
Offline-Update (Firmware) 387
Online-Update (Firmware) 384
Remote Storage 155, 159, 169, 300
Remote Storage Server 169
Remote-Installation des Betriebssystems 395
serielle Schnittstelle konfigurieren 50
Standard-DHCP-Name 34
Stromversorgung 218
über Server Configuration Manager konfigurieren 56
über Web-Oberfläche konfigurieren 54
Voreinstellungen 34
iRMC Advanced Features 374
iRMC Directory Service 367
Active Directory konfigurieren 369
eDirectory konfigurieren 371
OpenLDAP konfigurieren 371
iRMC DNS Registration 351
iRMC DNS Server 353
iRMC EMail Alerting 355
iRMC Firmware Settings 200
iRMC Information 196
iRMC LAN Interface 346
iRMC Mail Format Settings 358
iRMC SNMP Alerting 360
iRMC SSH Access 302
iRMC Telnet Access 302
iRMC User Management 361
iRMC-Benutzer erzeugen in OpenLDAP 131
iRMC-Benutzer der OU iRMCgroups zuordnen

in Active Directory 91
in eDirectory 120
in OpenLDAP 131
iRMC-Benutzer zuordnen 91, 120
iRMC-Benutzergruppe zuordnen 91, 120
iRMC-Benutzerverwaltung
global via Active Directory 80
global via eDirectory 98
global via OpenLDAP 127
in OpenLDAP integrieren 129
iRMC-Informationen abfragen 196
iRMC-Options, weitere 199
iRMC-Web-Oberfläche 181
Advanced Video Redirection (AVR) 292
Alerting 251
Alerting - Email Alerting 256
Alerting - Serial/Modem Alerting 254
Alerting - SNMP Trap Alerting 252
allgemeine Einstellungen 199
Aufbau der Bedienoberfläche 187
Benutzerverwaltung 64
Benutzerverwaltung (lokal) 263
Berechtigungen 184
BIOS Text Console 281
Certificate Upload 202
DHCP Configuration 247
Directory Service Configuration 273
DNS Configuration 249
Farbschema 199
Firmware-Einstellungen sichern 200
iRMC 195
iRMC Information 196
iRMC konfigurieren 54
iRMC SSH Access 302
iRMC Telnet Access 302
iRMC Telnet/SSH Zugang 302
Local Monitor 293
Network Interface 240
Network Settings 239
Ports and Network Services 243
Power Management 210
Power On/Off 211
Power Options 215
Power Supply Info 218
Remote Storage 300
Save iRMC Firmware Settings 200
Sensors 219
Sensors - Component Status 226
Sensors - Fans 220
Sensors - Power Supply 225
Sensors - Temperature 222
Sensors - Voltages 224
Server Management Information 233
Stromversorgung 218
System Component Information 191, 194
System Event Log 227
System Event Log Configuration 231
System Event Log Content 228
System Information 190
Temperaturanzeige 199
User Management 263
User Management - New User Configuration 265
User Management - User "name" Configuration 265, 266
iRMCgroups 76
iRMC-Benutzer zuordnen (eDirectory) 120
ISO Image (Image-File) 163, 169

K

kanal-spezifisch
Berechtigungsgruppe 62
Privilegien 62
Kommunikationsschnittstellen (iRMC) 21

Komponenten (Server)
überwachen 226
Konfiguration über Server Configuration Manager 333
Active Directory 369
ASR&R Fan Settings 342
ASR&R Temperature Settings 344
Benutzerkennung (iRMC User Manangement) 361
eDirectory 371
iRMC Advanced Features 374
iRMC Directory Service 367
iRMC DNS Registration 351
iRMC DNS Server 353
iRMC EMail Alerting 355
iRMC LAN Interface 346
iRMC Mail Format Settings 358
iRMC Networking Ports 349
iRMC SNMP Alerting 360
OpenLDAP 371
Systemkonfiguration starten 334
über Installation Manager aufrufen 334
über Operations Manager aufrufen 337
über Windows Startmenü aufrufen 335
Voraussetzung 333
Konfigurationstools, LAN-Schnittstelle 40
konfigurieren 355
Alarmbenachrichtigung 251
Alerting 55, 57, 251, 360
ASR&R Options 235
Benutzer 263, 265, 361
Benutzer (Details) 266
Benutzer, lokal 263, 361
Boot Options 213
Directory Service 273, 367, 369
Directory Service (Active Directory) 276
Directory Service (eDirectory) 278
Directory Service (Open LDAP) 278
Directory Service am iRMC 367
DNS für iRMC 249, 353
eDirectory 106, 371
eDirectory für LDAP 107
Ein- und Ausschalt-Zeiten (Server) 217
Email Alerting 256, 355
Ethernet-Einstellungen (iRMC) 240, 346
Host-Name für iRMC 247, 351
HP SIM-Integration 238, 375
IP-Parameter (iRMC) 346
iRMC 37
iRMC über Web-Oberfläche 54
Konsolumleitung 45, 281
LAN-Parameter (iRMC) 346
LAN-Schnittstelle 38, 41, 54, 56, 239
LDAP-Zugriff am iRMC 86
Mail-Format abhängige Einstellungen 261, 358
neuen Benutzer 265, 362
OpenLDAP 128, 371
Ports und Netzdienste (iRMC) 243, 349
Remote Storage Server 177
Serial/Modem Alerting 254
serielle Schnittstelle 50
Server Management Information 233
SNMP Trap Alerting 252
System Event Log (Server) 231
Text-Konsolumleitung 45, 281
Watchdog Settings 237
Konsolumleitung
bei laufendem Betriebssystem 48, 290
konfigurieren 44, 281
starten (Remote Manager) 326

L
LAN Interface 346
LAN-Parameter (iRMC)
konfigurieren 239, 346
LAN-Schnittstelle (iRMC) 39
konfigurieren 38, 41, 54, 56, 239
testen 43
LDAP Directory Service siehe auch Directory Service
LDAP siehe auch Directory Service
LDAP-Authentifizierungsprozess (eDirectory) 112
LDAP-Konfiguration 273, 367
Active Directory 276
eDirectory 278
OpenLDAP 278
LDAP-Zugriff (iRMC)
konfigurieren 86
LDIF-Datei 76
in Active Directory importieren 80
in Directory Service importieren 79
in eDirectory importieren 114
in OpenLDAP importieren 129
ldifde 81
License Key 137, 159, 197, 198, 199, 374
auf den iRMC laden 198
löschen 198
Linux, Remote-Installation 413
Local Monitor Off 141, 293
Local Monitor-Anzeige 293
lokale Benutzerkennung 59
lokale Benutzerverwaltung (iRMC) 64, 263, 361
lokaler Monitor, ein-und ausschalten 141, 293
Lüfter
testen 220
überwachen 220

M
Mail Format dependend Configuration 261
Mail Format Settings 358
Mail siehe auch Email und E-Mail
Management-Information 233
Management-Information siehe Server Management-Information
Maus-Umleitung (AVR) 144
Mauszeiger synchronisieren 144
Menü-Übersicht
Remote Manager 309
Microsoft Active Directory siehe Active Directory
Miscellaneous iRMC Options 199
Monitor, lokal 141, 293

N
NDS-Baum (eDirectory) erzeugen 106
Network 240
Network Interface 240
Network Settings 239
Networking Ports 349
New User Configuration 265
Novell ConsoleOne siehe ConsoleOne
Novell eDirectory Directory siehe eDirectory
Novell eDirectory Server siehe eDirectory Server
Novell eDirectory siehe eDirectory
Novell iManager siehe iManager

O
Offline-Update (Firmware) 387
Online-Update (Firmware) 384
Open LDAP Browser/Editor 82
OpenLDAP 18, 59, 68, 371
installieren 127
iRMC-Benutzer der OU iRMCgroups zuordnen 131
iRMC-Benutzer erzeugen 131
iRMC-Benutzerverwaltung 127

iRMC-Benutzerverwaltung
integrieren 129
iRMC-Gruppen und
Benutzerrechte 129
konfigurieren 128
Konfigurieren über Server Configuration Manager 371
LDIF-Datei importieren 129
Principal User erzeugen 130
SSL-Zertifikate erzeugen 127
Tipps zur Administration 132

P

Parallele AVR-Sitzungen 140
Passwort ändern 317
Ports and Network Services 243
Ports und Netzdienste für iRMC
konfigurieren 243, 349
Power Control 214
Power Management 210, 211, 215, 319
Power On/Off Time 217
Power Restore Policy 216
Restart-Optionen 214
Verhalten nach Stromausfall 216
Power On/Off 211
Power On/Off Time 217
Power Options 215
Power Restore Policy 216
Power Status Summary 212
Power Supply Info 218
Primary SMTP Server
Configuration 259
Principal User
in eDirectory erzeugen 116
in OpenLDAP erzeugen 130
privater DSA/RSA-Schlüssel
siehe DSA/RSA-Schlüssel
Privileges / Permissions 269
Privilegien siehe auch Berechtigung
Privilegien, kanal-spezifisch 62

R

RedhatFLBMC
Online-Update (Firmware) 385
Remote Manager 302, 307, 309
Anmeldeprozess 312
bedienen 309
Berechtigungen 316
Command Line Shell starten 327
Enclosure Information 321
Hauptmenü 314
Konsolumleitung starten 326
Menü-Übersicht 309
Passwort ändern 317
Power Management 319
Service Processor 325
System Eventlog 323
System Information 318
Remote Manager (Serial) 53
Remote Storage 155, 159, 169, 300
Gerätetyp 163
Speichermedien
bereitstellen 163
Speichermedien entfernen 168
Speichermedien verbinden 165
starten 161
Verbindung beenden 167
Remote Storage Server 169
als Service ausführen 175
Ausführungsmodus 175
Bedienoberfläche aufrufen 176
beenden 180
installieren 170
konfigurieren 177
stand-alone ausführen 175
starten 179
zuordnen 374
Remote-Installation des
Betriebssystems 395
generelles Vorgehen 396
Linux 413
Remote Storage-
Verbindung 398
Voraussetzungen 395

Windows 409
RemoteView Dokumentation 15
Restart-Optionen 214
RSA-Zertifikat siehe DSA/RSA-Zertifikat

S
Schnittstellen (iRMC) 21
Secondary SMTP Server Configuration 260
Secure Keyboard (AVR) 143
selbstsigniert, Zertifikat 208
Sensor
Farbcode 219
Status-Icon 219
überprüfen 219
Sensors 219
Serial/Modem Alerting 254
Serial/Modem Alerting konfigurieren 254
Serial/Modem-Schnittstelle (iRMC) 50
konfigurieren 51
Remote Manager (Serial) 53
Server
ASR&R Options 235
Ein- und Ausschalt-Zeit festlegen 217
ein- und ausschalten 214
Einstellungen konfigurieren 233
Eventlog einsehen 230
Eventlog konfigurieren 231
HP SIM Integration Options 238, 375
Komponenten überprüfen 226
Power Management 215
Power Management nach Stromausfall 216
Power Options 215
Power Supply Info 218
Remote-Installation (Linux) 413
Remote-Installation (Windows) 409
Remote-Installation des Betriebssystems 395
Sensoren überprüfen 219
über ServerView DVD 1 und konfigurieren 402
Watchdog Settings 237
Server Configuration Manager
Benutzerverwaltung 66
User Management (lokal) 361
Server configuration Manager
iRMC konfigurieren 56
Server Configuration Manager siehe auch Konfiguration über Server Configuration Manager
Server Management Information 233
Server Management-Information abfragen und konfigurieren 233
ServerView Update Manager Express siehe Update Manager Express
ServerView Update Manager siehe Update Manager
Service 15
Service Processor (Remote Manager) 325
Sicherheitsgruppe 73
Sicherheitsgruppe siehe auch Berechtigungsgruppe
SMASH CLP 328
Benutzerdaten 330
Kommando-Hierarchie 330
Kommandos 328
starten 327
Syntax 328
SMTP siehe auch Email und E-Mail
SNMP Alerting 360
SNMP Trap Alerting 252
konfigurieren 252, 360
SNMP-Alarmweiterleitung siehe SNMP Trap Alerting
Software Watchdog 237
Sondertasten, integrierte (AVR) 142
Spannungssensor überprüfen 224

Speichermedien
als Remote Storage verbinden 165
für Remote Storage bereitstellen 163
SSH 202, 302, 307, 309
SSL 202
SSL and SSH Certificate 202
SSL Copyright 134
SSL-Zertifikat
erzeugen 127
Standard-DHCP-Name (iRMC) 34
starten
Advanced Video Redirection 292
Remote Storage 161
Remote Storage Server 179
Remote Storage Server GUI 176
Status, Komponenten 226
Status-Icon
System Component Status 194
Status-Icon (Sensor) 219
stoppen
Remote Storage Server 180
Stromversorgung überprüfen 225
SuseFLBMC
Online-Update (Firmware) 385
synchronisieren, Mauszeiger 144
System Component Status
Status-Icon 194
System Event Log 227
Fehler-Icon 227
System Event Log
Configuration 231
System Event Log Content 228, 230
Fehler-Icon 227
System Eventlog 323
einsehen 230
Information 229
konfigurieren 231
System Fans 221
System Information 190, 191, 194
System Information (Remote Manager) 318
Systeminformationen abfragen 190, 318

T

Tastatur
umleiten (AVR) 140
virtuell (AVR) 143, 152
Tastenkombinationen, besondere (AVR) 142
Telnet 302, 307, 309
Temperatur überprüfen 222, 322
Temperature 222
Temperature Settings (ASR&R) 342, 344
Temperatursensor überprüfen 222
testen
LAN-Schnittstelle 43
Lüfter 220
Text-Konsolumleitung
bei laufendem Betriebssystem 48, 290
konfigurieren 44, 45, 281

U

überprüfen
Lüfter 220
Sensoren 219
Serverkomponente 226
siehe auch Enclosure Information 322
Spannung 224
Spannungssensor 224
Stromversorgung 225
Temperatur 222
Temperatursensor 222
überwachen siehe überprüfen
umleiten, Tastatur (AVR) 140
Umleitung der Maus (AVR) 144
Update Manager
Online-Update (Firmware) 384
Update Manager Express
Online-Update (Firmware) 385
Update, Firmware 377
USB Memory Disk 163

User "name" Configuration 266
User Information 267
User Management 263, 361

V
Verbindung
zu Remote Storage beenden 167
zu Remote Storage Server herstellen 301
zu Remote Storage Server trennen 301
verwalteter Server siehe Server
Verzeichnisdienst siehe Directory Service
Virtual Keyboard 143
virtuelle Tastatur (AVR) 143, 152
Voltages 224
Voraussetzung
AVR 138
iRMC-Konfiguration über Server Configuration Manager 333
Remote-Installation des Betriebssystems 395
Voreinstellungen, iRMC 34
vorkonfigurierte
Benutzerkennung 63

W
Watchdog Settings
konfigurieren 237
Web-Oberfläche siehe iRMC-Web-Oberfläche
Windows, Remote-Installation 409
WinFLBMB
Online-Update (Firmware) 385

X
X.509-Zertifikat siehe DSA/RSA-Zertifikat

Z
Zertifikat, selbstsigniert 208
Zertifizierungsstelle siehe CA 86
Zielgruppe 15
zuordnen
iRMC-Benutzer zu Gruppe 91, 120
Remote Storage Server zu iRMC 301, 374